

QUI FAIT LA LOI DANS LE CYBERESPACE ?

Jury de thèse

BRUNET Pierre, Professeur des universités en droit public
spécialisé en théorie du droit, Université Paris 1 – Panthéon
Sorbonne, Directeur de thèse

CASILLI Antonio, Professeur des universités en sociologie
spécialisé dans les usages numériques, Telecom Paris, Institut
Polytechnique de Paris

PREBISSY-SCHNALL Catherine, Maître de conférence en droit
public – Habilitée à diriger des recherches, spécialisée en droit des
nouvelles technologies de l'information et de la communication,
Université Paris Nanterre, Rapporteuse

PUJOLLE Guy, Professeur émérite en sciences informatiques
spécialisé dans les réseaux numériques, Université Pierre et Marie
Curie

WAGENER Noé, Professeur des universités en droit public
spécialisé dans les biens communs et le droit de l'immatériel,
Université Paris-Est Créteil, Rapporteur

ZOLYNSKI Célia, Professeure des universités en droit privé
spécialisée en droit de la propriété intellectuelle et en droit du
numérique, Université Paris 1 – Panthéon Sorbonne

Olivier BERLIN CLARÓS

23/04/2024

REMERCIEMENTS

Je remercie mon frère plus que quiconque pour m'avoir soutenu dans les épreuves que j'ai traversées durant cette thèse de huit ans. C'est à lui que je dois la force trouvée pour achever ce travail. Je remercie aussi ma belle-sœur qui n'a cessé de m'encourager dans ce doctorat, avec beaucoup de complicité, d'humour et d'humanité.

Je remercie ma mère pour m'avoir fait des retours après sa lecture de mon travail, et plus généralement mes parents d'avoir été disponibles pour moi, de s'être efforcés de m'aider, et de m'avoir accompagné dans certains moments difficiles.

Je remercie mon directeur de thèse, Pierre Brunet, qui a su me laisser la liberté nécessaire à ma méthode de travail, et me donner les bons conseils pour corriger les erreurs de rigueur dans ma thèse.

Je remercie mes amis Samy, Louis et Célia pour leur présence, leur patience, et leur soutien appuyé lorsque j'en avais besoin.

Je remercie beaucoup les étudiants de Créteil et de la Sorbonne à qui j'ai eu plaisir d'enseigner. Je me suis épanoui dans le lien humain que j'ai partagé avec un certain nombre d'entre eux. Ils m'ont rendu une certaine confiance en l'humanité, qui m'a encouragé à reprendre la rédaction de la thèse.

Enfin, je remercie mon ex-partenaire pour l'aide qu'il m'a apportée dans la réalisation de trois schémas figurant dans la thèse, et pour l'intérêt qu'il a prêté à mes travaux.

SOMMAIRE

Première Partie – L'étude des rapports de force interhumains en ligne

Sous-Partie 1. L'identification des rapports de force en ligne par les États et chercheurs

Chapitre 1. La conception exogène du réseau internet

Chapitre 2. La conception endogène du réseau internet

Sous-Partie 2. La clandestinité (scientifico-étatique) des prescriptions numériques

Chapitre 1. Le caractère prescriptif des données numériques

Chapitre 2. Le mode prescriptif numérique des données en ligne

Deuxième Partie – La régulation des rapports de force interhumains en ligne

Sous-Partie 1. Techniques basiques de restriction de l'accès à internet

Chapitre 1. Introduction à la régulation d'internet

Chapitre 2. Les techniques de blocage et de filtrage de l'accès

Sous-Partie 2. Étude de l'efficacité régulatrice sur internet

Chapitre 1. La technique de la centralisation du réseau

Chapitre 2. Évaluation de l'efficacité de l'action régulatrice sur internet

INTRODUCTION

I. Le corpus juridique

On introduit cette thèse très classiquement, en informant le lecteur de notre conception du « droit ». Notre regard sur le droit est d'abord celui d'un positiviste, qui n'admet dans le corpus juridique que les règles et principes posés par l'être humain (droit positif), et qui exclut de ce corpus les règles et principes que l'être humain voudrait voir posés (droit naturel). Or, comment identifier une règle posée *juridiquement* ? Une règle peut être posée socialement, telle une personne qui pose des limites à son ami en le sanctionnant par une rupture de la relation si les limites ne sont pas respectées par cet ami. Elle peut être posée économiquement (un(e) chef d'entreprise qui pose des règles de détermination des salaires ou de répartition de son budget), religieusement (un imam qui, interprétant le Coran, pose des règles et principe comportementaux aux croyants), dans la sphère familiale (un parent qui pose une interdiction, une obligation ou une permission à son enfant) etc.

On considère qu'une règle ou un principe est posé juridiquement s'il est produit par la personne publique — pouvoir exécutif, législatif ou juridictionnel —, ou s'il est produit par une personne habilitée par la personne publique à poser juridiquement une règle ou un principe. On évalue donc le caractère juridique d'une règle ou d'un principe d'après sa source de production. Cette position nous conduit à délimiter le périmètre du « **droit** », en y incluant **toute règle et tout principe posé par la personne publique ou par une personne habilitée par la première à produire du droit**.

On appelle « normes juridiques » les significations des règles et principes ainsi posés. Ce concept de norme juridique a été largement popularisé, en droit, sous l'influence du juriste autrichien Hans Kelsen depuis les années 1930. Pour Kelsen, le droit est composé de normes, qu'il définit comme des « *significations d'un acte de volonté* »¹. L'idée selon laquelle un acte juridique résulte d'un acte de volonté est antérieure aux écrits de Kelsen. Les positivistes de la fin du XIXe siècle (Georg Jellinek, René Carré de Malberg...) s'opposaient déjà largement à l'École des exégètes, pour qui le juge se cantonnait à faire application de la loi sans l'interpréter. Ces positivistes soutenaient alors que l'État possède une volonté propre, qu'il exprime chaque fois qu'il pose une règle de droit.

Les arguments positivistes ont trouvé un prolongement avec l'École réaliste qui a émergé dans les années 1950-1960. L'École réaliste française considère que l'interprétation du juge résulte d'un acte de volonté (le juge interpréterait la règle selon sa réalité personnelle) et non d'un acte de connaissance (le juge ne s'affranchirait pas de la lettre de la règle)². L'une des critiques dirigées contre cette théorie peut se résumer ainsi : si son intention subjective est le seul critère du juge, si tout peut n'être que caprice du juge, comment expliquer la cohérence des décisions de justice ? Comment expliquer ne serait-ce que le phénomène de la jurisprudence ? En réponse à ces questions, le réaliste Michel Troper leur objecte le cas du joueur d'échecs qui, conséquemment à l'ensemble des coups joués par son adversaire et par lui-même, se trouve à un moment contraint de déplacer telle pièce de l'échiquier de telle manière pour éviter la défaite. Il ne peut pas déplacer une autre pièce et il ne peut pas la déplacer d'une autre manière sans

¹ KELSEN Hans, *Théorie pure du droit*, 2^e édition, Paris, PUF, 1996, p. 2-3

² À toutes fins utiles, Riccardo Guastini rappelle que le débat sur l'interprétation n'est pas dual mais que, à cette première opposition entre doctrines « littéraliste » et « intentionnaliste », s'ajoutent celle entre doctrines « statique » et « dynamique » : GUASTINI Riccardo, *Leçons de théorie constitutionnelle*, Dalloz, 2010, p. 214s.

être mis en échec. « *La contrainte ne vient pas de l'extérieur du jeu : sa condition psychologique, sa religion, son idéologie sont indifférentes* » ; seuls les coups joués jusqu'à présent en application des règles du jeu sont déterminants, de sorte que la contrainte est interne au « *système des échecs* » lui-même³. De la même façon, le juge serait engagé dans un système du Droit qui le contraindrait à rendre certaines décisions d'une certaine manière du seul fait qu'il participe au « jeu » juridique. Tout comme le joueur d'échecs est libre de déplacer les pièces selon sa volonté, le juge est libre d'interpréter une règle de droit selon sa volonté. Mais pour l'un comme pour l'autre aussi, leur liberté se heurte toujours à la cohérence exigée par leur système d'appartenance (échecs ou droit). La cohérence des décisions de justice ne remet dès lors pas en cause l'intention du juge comme source principale de sa décision. Cette intention est seulement objectivée par ce que le juge « *ressent* » comme un « *système social* »⁴ de fait au sein du Droit.

L'explication volontariste des actes juridiques ne remonte donc pas à Kelsen : elle existait avant lui, après lui, et indépendamment de lui. Cependant, l'apport de Kelsen sur ce point fut de définir la norme comme *la signification* de l'acte de volonté qui pose un devoir-être, c'est-à-dire la signification issue l'acte « *par lequel quelqu'un veut que quelque chose "doit avoir lieu"* »⁵. Dans ce cadre, **la norme** ne **désigne** pas l'acte de volonté lui-même (par exemple l'adoption de la loi), mais **la signification d'un devoir-être issu de cet acte** (p. ex. la signification de la loi). Cependant, la doctrine a déjà démontré que certaines normes juridiques ne résultent pas d'un acte de volonté identifiable⁶. On ne retiendra donc pas le critère de la volonté comme une spécificité de la norme juridique, et on définira alors **la norme** comme **la signification d'un devoir-être posé par une règle ou un principe**. La norme juridique est celle posée par les sources de production qu'on a déjà décrites (personne publique, ou personne habilitée par la personne publique à produire du droit).

Cette définition en appelle deux autres : celle de la règle ; et celle du principe. Premièrement, notre conception de la règle est largement inspirée d'un article du réaliste scandinave Alf Ross. Dans sa célèbre analogie du *Tû-tû*⁷, il s'intéresse à une règle tribale qui soumet à une cérémonie de purification celui frappé par la malédiction du *tû-tû* pour avoir affronté sa belle-mère, tué un animal totémique ou mangé la nourriture préparée pour le chef. Comparant cette règle tribale avec la règle de droit, il observe qu'elles partagent la même structure. À l'image de la règle tribal, la règle de droit consiste à systématiser un lien causal entre un fait de conditionnement (qui déclenche l'exécution de la règle) et une conséquence de la règle (qui sanctionne l'application de la règle). Ainsi :

³ TROPER Michel et CHAMPEIL-DESPLATS Véronique, « Introduction » in TROPER M., CHAMPEIL-DESPLATS V. et GRZEGORCZYK Christoph (dir.), *Théorie des contraintes juridiques*, LGDJ, Bruylant, 2005, p. 2-3

⁴ MILLARD Éric, « Le réalisme scandinave et la théorie des contraintes » *in ibid.*

⁵ MILLARD Éric, « Qu'est-ce qu'une norme juridique ? », *Cahiers du Conseil constitutionnel*, n° 21, janv. 2007. V. aussi directement la définition de Kelsen de la norme comme « *la signification que possèdent certains actes humains qui, selon l'intention de leurs auteurs, visent à provoquer une conduite d'autrui* » (KELSEN H., *Théorie pure du droit*, préc., p. 7)

⁶ Par exemple, « *un commandement est imputable à une personne, la coutume ne l'est pas ; un commandement est un acte intentionnel, la coutume ne l'est pas. Un commandement est une action délibérée, voulue ; une coutume n'est pas un acte voulu : c'est plutôt un acte subi* » (LA TORRE Massimo, « Le modèle hiérarchique et le Concept de droit de Hart », *Revus*, n° 21, 2013, p. 117-139)

⁷ ROSS Alf, « *Tû-Tû* », *Harvard Law Review*, vol. 70, 1957, p. 812-825

Si j'achète une maison, alors la personne qui y pénètre sans mon autorisation sera punie
 Fait de conditionnement (F) Lien causal Conséquence de la règle de droit (C)

Si un membre de la tribu tue un animal totémique, alors il devra subir une purification
 Fait de conditionnement (F) Lien causal Conséquence de la règle tribale (C)

On en déduit, d'une part, que **toute règle peut s'écrire par la structure $F \rightarrow C$** , où F désigne le fait de conditionnement qui provoque la conséquence C , et où $\rightarrow$ désigne le lien causal (« alors ») grâce auquel l'intervention du fait F engendre la conséquence C . D'autre part, plusieurs règles peuvent être rangées dans une même catégorie, de façon que cette catégorie implique toutes les règles qu'elle couvre. Par exemple, la catégorie « propriété » permet de faire découler la même conséquence C (« la personne qui pénètre dans ma maison sans mon autorisation sera punie ») de plusieurs faits F différents (« si j'achète une maison », « si la maison m'est donnée par son propriétaire », « si j'occupe la maison continuellement, paisiblement, publiquement, sans équivoque et en me comportant comme son propriétaire depuis un long terme »). Ou encore, la catégorie « tû-tû » permet de faire découler la même conséquence C (« la personne devra subir une purification ») de plusieurs faits F différents (« si un membre de la tribu tue un animal totémique », « si un membre de la tribu affronte sa belle-mère », « si un membre de la tribu mange la nourriture préparée pour le chef »). De même, la catégorie « propriété » permet de justifier une diversité de règles $F \rightarrow C$ (« si une personne vole mes biens, elle encourt telle peine de prison », « si une personne consomme une oeuvre de l'esprit dont je suis l'auteur, elle encourt telle amende », « si une personne se fait passer pour le propriétaire de mes biens pour contracter des dettes à mon nom, elle encourt telle autre sanction »...). De cette façon, invoquer une catégorie permet d'appliquer les « séries de règles »⁸ qui s'y rattachent.

On peut ainsi définir la règle comme l'existence d'un rapport causal entre un fait de conditionnement et une conséquence provoquée par la survenance de ce fait. Il faut encore distinguer deux types de règles, aujourd'hui bien connues des juristes : la règle rigide ; et la règle souple. La règle rigide est celle qu'on a déjà décrite sous le nom de « règle », qui se caractérise par une applicabilité systématique de la conséquence C en présence du fait F ⁹. A contrario, la règle souple se caractérise par le fait que la conséquence C est optionnelle, dans son application et/ou dans ses propositions. La règle souple peut donc s'écrire $F \rightarrow (C)$. Par exemple, « si une entreprise s'est engagée à telle action ou inaction (F), alors il est préférable qu'elle respecte son engagement (C) » (formulation-type des codes de conduites auxquels souscrivent les entreprises) ; « si une entreprise embauche tel effectif ou totalise tel chiffre d'affaire, alors il est préférable qu'elle agisse de telle ou telle façon et/ou [option] qu'elle n'agisse pas de telle ou telle façon » etc.

On examinera *infra* un peu plus en détail le « droit souple », mais on peut déjà en tirer des conséquences sur le concept de « règle contraignante ». On distingue deux types de contraintes : la contrainte abstraite ; et la contrainte concrète. La contrainte abstraite désigne l'applicabilité systématique d'une conséquence C lorsqu'intervient le fait de conditionnement F . Une règle est donc abstraitement contraignante si elle s'impose hypothétiquement dans le ressort de son destinataire. La contrainte abstraite résulte du *pouvoir de contraindre*, c'est-à-dire la possibilité d'assortir F d'une conséquence C systématiquement applicable, ou bien la possibilité d'exiger

⁸ *Ibid.*, p. 820

⁹ On parle bien d'*applicabilité* systématique, et non d'*application* systématique. La conséquence C d'une règle rigide est systématiquement applicable, mais elle n'est pas systématiquement appliquée.

l'application de cette conséquence chaque fois que F est rempli. Par exemple, le législateur et le juge exercent leur pouvoir de contraindre en émettant une loi ou une décision de justice qui s'applique hypothétiquement, jusqu'à ce que la conséquence prévue par la loi ou la décision soit réellement mise en oeuvre dans le ressort du destinataire.

Quant à la contrainte concrète, elle désigne l'application d'une conséquence C lorsqu'intervient le fait de conditionnement F. La contrainte concrète résulte de la *contrainte effective*, c'est-à-dire la mise en application de la conséquence C dans le ressort (physique, psychique, patrimonial, familial...) du destinataire de la règle. Par exemple, un administré sommé par les services fiscaux de payer des arriérés est contraint abstraitement par l'injonction administrative de verser les pénalités de retard ; il peut refuser de payer, s'acheter une nouvelle identité, fuir le pays, et ne sera pas contraint concrètement à régler les sommes dues, il restera seulement contraint abstraitement par cette obligation ; il ne sera contraint concrètement de le faire qu'au moment même où il le fait réellement sur injonction administrative. De même, un prévenu condamné à purger une peine de prison sur décision du juge ne sera contraint concrètement par cette décision qu'une fois emprisonné effectivement, tout comme une personne est contrainte concrètement par la règle « tu ne tueras point sinon tu seras puni » aussi longtemps que cette personne s'interdit effectivement de tuer pour respecter cette règle. En ce sens, une règle souple n'est certes pas contraignante abstraitement (car la conséquence C n'est pas systématiquement applicable), mais elle peut être contraignante concrètement (car les destinataires de la règle souple peuvent s'obliger à la respecter).

On parlera de *prescriptions* pour désigner essentiellement les règles rigides. En effet, on appelle « prescription » l'ordre (général ou particulier) de faire appliquer une règle exécutable. On reconnaît à la prescription la particularité de conserver son effet contraignant après son édicton. Ceci est valable pour les prescriptions incarnées aussi bien par une règle rigide que par une règle souple. Cependant, une règle rigide étant abstraitement contraignante, elle est systématiquement exécutable et comporte implicitement ou explicitement l'ordre d'être faite appliquée. Du fait de la contrainte abstraite qui l'accompagne, l'existence contraignante de la règle rigide persiste donc après son édicton. A contrario, une règle souple ne peut être que concrètement contraignante si elle est respectée par ses destinataires, mais la conséquence C n'est pas systématiquement applicable chaque fois que le fait F est rempli. Si la conséquence C d'une règle souple est appliquée dans un litige où le fait F intervient, elle devient une règle rigide dans le seul cadre de ce litige, et peut exceptionnellement être qualifiée de prescription dans ce cadre. De même, tant que les destinataires se sentent obligés pour une raison ou pour une autre de respecter la règle souple, elle les contraint concrètement mais pas abstraitement car la conséquence C n'est pas systématiquement applicable. Par conséquent, la prescription incarnée par une règle rigide est une prescription en soi, en toutes circonstances, car son effet contraignant persiste après l'édiction de la règle exécutable. En revanche, la prescription incarnée par une règle rigide n'est une prescription que dans la mesure où ses destinataires s'obligent à la respecter, ou dans la mesure où la conséquence C est faite appliquée dans un cas concret.

Deuxièmement, outre les règles, qu'en est-il des principes ? L'une des définitions les plus célèbres est proposée par le réaliste américain Ronald Dworkin. Dworkin distingue lui aussi la règle du principe. D'après lui, la règle est valide si ce qu'elle prescrit est appliqué. Il en déduit que la règle tient sa validité d'un choix binaire : soit les conditions prescrites par la règle sont remplies (auquel cas la règle est valide) ; soit elles ne le sont pas (et la règle n'est pas valide). À l'inverse,

le principe ne procède d'aucune binarité : s'il est mobilisé par le juge, c'est qu'il est valide. Dworkin et ses partisans comme Robert Alexy¹⁰ en déduisent l'équation suivante : si deux règles se contredisent, l'une est évacuée au profit de l'autre ou, au contraire, elle constitue une exception à l'autre. Lorsque deux règles sont en conflit, le conflit est donc résolu en jouant sur la *validité juridique* de l'une ou de l'autre, c'est-à-dire sur l'application ou l'inapplication d'une règle par le juge dans le cas concret. En revanche, si deux principes se contredisent, il est impossible de jouer sur leur validité qui est déjà acquise ; le conflit sera alors résolu en jouant sur leur *valeur juridique*, c'est-à-dire sur leur positionnement hiérarchique, leur « *importance* », leur « *poids* ». Si des principes se contredisent, le juge n'en évincera aucun ; il mettra les principes en balance, les pèsera¹¹.

Notre conception des principes est plus large que celle de Dworkin. On définit le principe normatif (ci-après « principe ») comme **la signification qui fonde l'interprétation d'une règle**. Toute règle est interprétée selon un ou plusieurs principes. Cela implique qu'il n'existe pas de règle sans principe. De la même manière, il n'existe pas de principe normatif sans règle. Si le principe qui fonde la règle disparaît, la règle disparaît à son tour. En ce sens, la règle est le moyen par lequel le principe est mis en œuvre. Par exemple, un juge peut être guidé dans son interprétation par des principes moraux. De même, la loi repose sur des principes moraux ou idéologiques. Plus récemment, le juge a consacré des principes « juridiques » dont la seule particularité, par rapport aux autres principes normatifs, consiste à bénéficier d'une valeur juridique (*i.e.* d'une position plus ou moins fixe dans la hiérarchie des normes) en plus d'être posés par la personne publique ou une personne habilitée par la première.

Un même principe peut fonder l'interprétation de plusieurs règles. Par exemple, le principe moral « il est injuste de voler autrui » (P_M) peut fonder les règles juridiques « condamnation pénale du voleur » (R_1) et « réparation civile du préjudice de la victime » (R_2). En supposant que ce principe fonde uniquement ces deux règles et aucune autre, le principe moral $P_m = \langle R_1; R_2 \rangle = \langle (F_1 \rightarrow C_1); (F_2 \rightarrow C_2) \rangle$. Bien qu'on illustre ici ce principe avec deux règles rigides, un même principe peut aussi bien fonder des règles rigides que des règles souples.

Si un même principe peut certes fonder plusieurs règles, il est tout aussi vrai qu'une même règle peut se retrouver dans plusieurs principes. Dans ce cas, l'effondrement d'un seul principe qui contient la règle n'engendre pas l'effondrement de la règle elle-même, qui reste contenue dans d'autres principes. Par exemple, la règle R_1 (condamnation pénale du voleur) peut se retrouver à la fois dans le principe moral « il est injuste de voler » (P_M) et dans le principe économique « le vol représente une perte d'argent nocive pour le marché » (P_E). Si plus personne n'adhère à ce principe moral, il est toujours possible d'adhérer au principe économique qui fonde l'interdiction du vol, et la règle interdisant le vol se maintiendra alors à travers P_E . Dès lors que le principe fonde la règle, le premier est nécessairement supérieur à la seconde qui en dépend¹².

¹⁰ ALEX Y Roberts, *A Theory of Constitutional Rights*, Oxford University Press, 2002 [publication originale en allemand en 1986], p. 47-50

¹¹ Sur cette théorie de Dworkin, v. *Ibid.* et DWORKIN Ronald, « The Model of Rules », *University of Chicago Law Review*, vol. 35, 1967, p. 14-46

¹² Ainsi, pour ce qui est des principes juridiques, le principe général du droit (PGD) a la valeur juridique de la norme qui le révèle, tout comme le principe fondamental reconnu par les lois de la République (PFR LR) a une valeur supra-législative alors qu'il est déduit d'une loi

En somme, on considère que le corpus juridique (positif) est à ce jour constitué de trois types de normes — règles de droit rigides, règles de droit souples et principes juridiques — qui peuvent être ainsi notées :

Règle rigide (R_R) = $F \rightarrow C$

Règle souple (R_S) = $F \rightarrow (C)$

Principe = $\langle F \rightarrow C \rangle$ ou $\langle F \rightarrow (C) \rangle$

Ces trois types de normes juridiques constituent donc le corpus juridique sur lequel on s'appuiera tout au long de cette thèse. On s'efforcera de porter un regard axiologiquement neutre sur le corpus juridique de chaque pays comparé dans cette thèse, c'est-à-dire sans inclure nos valeurs idéologiques et morales dans l'étude de ces différents corpus et sans nous appuyer sur ces valeurs pour en tirer nos conclusions.

II. Enjeux étudiés

La délimitation du corpus juridique est d'autant plus inévitable quand on s'interroge sur l'efficacité ou l'inefficacité *des* normes juridiques (en général) pour réguler le réseau internet. C'est précisément l'objet de cette thèse. On distingue l'ineffectivité et l'inefficacité du droit positif. **On appelle « ineffectivité du droit positif » le défaut d'application d'une norme juridique.** Cela couvre diverses hypothèses, comme l'invalidation d'une règle par le juge (écartée dans un cas concret), l'inapplication d'une règle pénale par la police judiciaire ou d'une règle administrative par l'administration, le passage sous silence d'une règle jamais invoquée, méconnue ou d'une vieille règle jugée dépassée par la modernité... Dans toutes ces situations, la règle est ineffective en ce sens qu'elle ne produit pas les effets qu'elle prescrit lorsque survient le fait de conditionnement mentionné par la règle.

On appelle « inefficacité du droit positif » l'insatisfaction des objectifs recherchés par la règle. Une loi proscrivant la consommation de radis sera effective si les acteurs chargés de son exécution ou de son application (juge, police...) l'exécutent ou l'appliquent réellement, mais elle sera inefficace si elle n'entraîne pas une baisse de la consommation de radis. Inversement, une loi qui obligerait les hébergeurs à censurer les contenus « âgistes » (propos discriminants en raison de l'âge) et condamnerait pénalement les utilisateurs qui publient ce type de contenus, une telle loi serait ineffective si le juge, lors de son contrôle de proportionnalité, en écartait chaque fois l'application au profit de la liberté d'entreprise des hébergeurs et de la liberté d'expression des utilisateurs ; elle pourrait néanmoins être efficace si, par peur fantasmée de la sanction pénale, les utilisateurs cessaient de produire des contenus âgistes. Ainsi, une règle s'applique *effectivement* si elle est faite respectée ; elle s'applique *efficacement* si elle débouche sur le résultat escompté. L'efficacité fait alors oublier l'exécution de la règle (son interprétation) derrière son application concrète (son respect réel par les destinataires de la règle, l'atteinte de l'objectif recherché par la règle). Dans le cadre de cette thèse, on questionne exclusivement l'efficacité des normes juridiques auprès des comportements observés internet, et non leur ineffectivité.

On verra que le problème de l'efficacité de la régulation juridique d'internet passionne de nombreux chercheurs depuis plusieurs décennies¹³. Dans notre cas, l'irrésolution actuelle de ce problème défie bien sûr notre désir de le résoudre, mais notre intérêt pour le sujet dépasse cette simple curiosité. On a choisi de traiter ce sujet car trois de ses principaux enjeux ont stimulé notre intérêt.

Le premier d'entre eux est celui de l'impuissance des États¹⁴. On a vu que l'État est la source fondamentale du droit moderne d'après notre définition des normes juridiques. Dans ces conditions, l'impuissance de l'État peut-elle engendrer sa disparition, et celles des normes juridiques modernes (posées par l'État ou une personne habilitée par lui) ? L'anéantissement de la structure étatique en raison de son impuissance nous semble possible théoriquement, mais une telle issue par étapes, et paraît peu probable à ce jour. La première étape vers l'effondrement d'une structure étatique est sa perte de souveraineté. Une régulation étatique absente ou inefficace d'internet peut nuire doublement à la souveraineté de l'État. Elle peut d'abord engendrer la naissance d'un espace public de sociabilité (le réseau internet) dans lequel l'État a peu voire aucune autorité, alors que sa population peut y subir des dommages (propos haineux, violations de droits d'auteur, vols de données...) et que ses intérêts peuvent s'y trouver menacés (divulgaration de secrets d'État, cyberattaques contre les opérateurs d'importance vitale ou de services essentiels, organisations et propagandes terroristes, fausses informations délégitimant un État ou altérant le processus électoral...). Une régulation déficiente d'internet peut ensuite provoquer la dépendance technologique, économique et géopolitique d'un État à d'autres États. Seulement, cette perte de souveraineté ne peut mener à l'anéantissement de l'État que si elle est généralisée, c'est-à-dire si la population régie par l'État ne répond plus de ses normes juridiques quel que soit le secteur d'appartenance des membres de cette population (relations sociales, économie, numérique, religion...).

Même lorsque la perte de souveraineté étatique est généralisée, cela n'implique pas encore la disparition de l'État. Rien n'empêche l'État impuissant de continuer à fonctionner, de continuer à édicter des normes juridiques et de les faire appliquer pour les rendre effectives — de la même manière qu'un être humain qui se sent impuissant après une série d'échecs peut continuer à vivre malgré son sentiment d'impuissance, dans l'espoir notamment de retrouver une part de pouvoir sur le réel. Pour que l'État s'effondre, une seconde étape est donc requise en plus de la perte de souveraineté : l'abandon de son existence par l'État, son suicide en quelque sorte (tout comme certains Empires, lors des Traités de Westphalie de 1648, ont abandonné leur existence au profit d'États délimités par des frontières fixes et soumis aux principes d'égalité souveraine et de non-ingérence) ; ou bien la destruction de toute capacité de l'État à produire du droit, son meurtre (par exemple dans le cadre de la conquête d'un État par un autre qui l'annexe). Aussi longtemps que l'État souhaite se maintenir, et aussi longtemps qu'il peut produire du droit, il se maintiendra quel que soit son niveau de puissance ou d'impuissance. On voit mal comment le réseau internet pourrait détruire les capacités des États à produire du droit, mais les États peuvent en revanche se

¹³ Tels David Post et David Johnson, Lawrence Lessig ou encore, dans une certaine mesure, Yochai Benkler pour ne citer que les plus connus, dont on détaillera les théories plus loin dans la thèse

¹⁴ Par exemple, « *une très grande part de la régulation du Réseau internet est produite, mise en œuvre, et même sanctionnée en dehors de l'emprise des États* » (AUBY Jean-Bernard, « Autorégulation et droit administratif », *Droit Administratif* n° 8-9, Jurisclasseur, 2008). V. Aussi ITEANU Olivier, *Quand le digital défie l'État de droit*, Eyrolles, 2016. Ou encore, selon l'ancien secrétaire d'Etat chargé du numérique, Mounir Mahjoubi, l'article 3 du projet de loi renforçant la lutte contre les violences sexistes et sexuelles (loi réprimant le harcèlement en ligne) « *permettra (...) de réaffirmer qu'internet et les réseaux sociaux ne se situent pas en-dehors des lois de la République* » (réponse, publiée au JO le 12 juin 2018, à la question au gouvernement n° 6340, Assemblée Nationale).

« suicider » s'ils ne parviennent pas à dépasser leur impuissance sur internet. Surtout, comme on l'a déjà souligné, l'État ne peut abandonner son existence par impuissance que si sa perte de souveraineté est généralisée, de sorte que le réseau internet ne peut pas à lui seul provoquer l'impuissance totale de l'État (à moins qu'internet devienne la source exclusive des règles respectées par la population de cet État).

Si l'État s'effondre par impuissance, internet y aura probablement contribué plus qu'il ne l'aura provoqué à lui seul. Enfin, on constatera dans cette thèse que le réseau internet peut être étatisé, et que les États avancent de plus en plus dans cette voie. Cette étatisation n'est pas gage d'efficacité des normes juridiques auprès des comportements en ligne, mais elle offre à l'État un contrôle et une présence sur internet qui ne présagent aucun « suicide » de la structure étatique. Pour toutes ces raisons, on pense que la disparition des États due à leur impuissance sur internet n'est pas à l'ordre du jour. Reste qu'internet demeure un vrai défi pour la souveraineté des États comme on l'a illustré.

Au-delà de l'impuissance des États, le deuxième enjeu qui nous a attiré vers ce sujet réside dans l'échelle de diffusion que peuvent acquérir les données sur internet. D'une part, des entreprises peuvent contrôler les informations accessibles à des milliards de personnes. Ainsi, on verra plus loin qu'on estime à 3,7 milliards environ le nombre d'utilisateurs uniques mensuels du moteur de recherche Google Search au dernier semestre 2022. Cela signifie que, à travers son service Google Search, la société Alphabet peut imposer ses décisions politiques à 3,7 milliards de personnes dans le monde (politiques de confidentialité et de sécurisation des données personnelles de utilisateurs, politiques de censure des contenus, de valorisation des contenus, des outils mis à disposition des utilisateurs et des annonceurs...). Cela signifie par-là même qu'elle contrôle les informations auxquelles peuvent accéder 3,7 milliards de personnes sur son service.

D'autre part, les dommages nés via internet peuvent eux aussi obtenir une échelle de diffusion vertigineuse. D'un côté, par exemple, plusieurs centaines voire milliers de personnes peuvent simultanément harceler une même victime. De l'autre côté, une seule personne peut diffuser un logiciel malveillant auprès de plusieurs milliers de personnes. Dans les deux cas, le dommage se diffuse auprès de milliers de machines différentes en quelques secondes. Si les dommages concomitants et à grande échelle ont toujours existé dans l'espace physique, ils peuvent désormais acquérir leur échelle de diffusion *en-dehors de l'espace physique*. Les dommages se diffusent dans un *cyberespace*, qu'on définit comme l'ensemble des mémoires informatiques (disques durs, mémoires vives...) connectées à internet.

Certes, les dommages sont ressentis physiquement par les victimes. Certes, les mémoires informatiques existent sur un support physique, et obéissent aux lois de la physique. Mais ces dommages naissent de données stockées dans les espaces mémoire connectés à internet, et ne se diffusent que par le stockage et l'exécution de ces données. Or, les règles qui déterminent la diffusion d'une donnée dans le cyberespace sont-elles les mêmes que les règles qui déterminent la diffusion d'une action dans l'espace physique ? Sous quelles conditions une donnée acquiert-elle une vaste échelle de diffusion, et sous quelles conditions perd-elle son échelle de diffusion ? Comment expliquer la difficulté à contrôler l'échelle de diffusion d'une donnée dans le cyberespace ? Ces questions, et surtout les réponses qu'on proposera dans la thèse, révèlent la particularité incarnée par internet dans la diffusion des dommages.

Enfin, le troisième enjeu qui nous a fasciné est celui de la contrainte *interne* à la machine numérique. On appelle « contrainte interne à la machine numérique » tout ce qui oblige la

machine à stocker ou à supprimer des données dans sa mémoire, et tout ce qui oblige la machine à exécuter les données stockées. Deux types de composants internes à la machine sont dans ce cas contraints - la mémoire qui stocke ou supprime les données, et le processeur qui les exécute. On identifie quatre manières de générer une contrainte interne à la machine. Les trois premières découlent de l'applicabilité et de l'application des règles physiques (1^{ère} manière), mécaniques (2^e manière) et/ou électriques (3^e manière) dont dépend le fonctionnement de la machine. Ainsi, la machine peut être contrainte à supprimer certaines données si, par exemple, l'utilisateur fait tomber son smartphone et en altère les capacités mémoire. Dans ce cas, des données peuvent être supprimées sans que l'utilisateur ait produit une requête ordonnant la suppression de données. Ou encore, la machine peut être contrainte à supprimer toutes les données qu'elle stocke si un utilisateur la détruit en la manipulant. Par exemple, un salarié fraîchement licencié qui dirige sa rage contre les ordinateurs de son entreprise en les cassant les uns après les autres exerce un pouvoir contraignant sur ces machines, et donc sur une fraction du réseau internet (celle constituée par les ordinateurs connectés à internet ainsi détruits).

Dans le cas du smartphone tombé, la contrainte de la machine par l'être humain résulte de l'applicabilité systématique de la conséquence C dans la règle : « *si j'abîme la mémoire vive d'un smartphone (F), alors seront supprimées les données stockées dans la partie affectée de la mémoire (C)* ». Dans le cas des ordinateurs cassés, la contrainte résulte de l'applicabilité systématique de la conséquence C dans la règle : « *si je détruis la mémoire vive et le processeur d'un ordinateur (F), alors les données stockées sur l'ordinateur seront supprimées et la machine sera incapable de traiter des requêtes (C)* ». Dans les deux cas, la contrainte exercée par l'être humain sur la machine résulte de l'applicabilité de règles physiques, électriques et mécaniques.

La quatrième manière de contraindre une machine numérique consiste à produire des données binaires (i.e. des données sous la forme de 0 et de 1). Toute production de données binaires contraint la machine, soit à stocker des données exécutables, soit à ordonner l'exécution de données. Il est vrai que la production de données binaires résulte fondamentalement de lois physiques, électriques et mécaniques. On verra cependant que ces données binaires sont porteuses de règles propres, qui n'existent pas parmi les lois physiques, électriques ni mécaniques. Par exemple, le programmeur, i.e. le créateur d'un logiciel, peut stocker la règle (abstraction donc hypothétiquement contraignante) : « *si un utilisateur marque un contenu par un "like" (F), alors le contenu ainsi marqué figure publiquement parmi tous les contenus aimés par l'utilisateur (C)* » ; ou inversement « *si un utilisateur marque un contenu par un "like" (F), alors ce contenu apparaît ainsi marqué dans l'espace privé et non public de l'utilisateur (C)* ». De même, l'utilisateur peut ordonner l'exécution de cette règle programmée dans le cadre d'une requête exécutée par le processeur de la machine, alors contraint concrètement à exécuter cette requête portant la règle. On aura l'occasion d'illustrer plusieurs de ces règles particulières qui résultent de la production de données binaires, et qu'on qualifiera de « prescriptions numériques ».

Ces règles (rigides) qui n'existent que dans le cyber-espace, et leur application par le processeur de la machine numérique, sont à l'origine des rapports de force inter-humains qui se jouent directement dans le cyberspace. La contrainte suscitée par les prescriptions numériques, bien qu'interne à la machine, semble donc provoquer des conséquences externes à la machine sur les rapports de force inter-humains. On expérimentera cette hypothèse pour la

vérifier ou l'infirmer. Notre thèse survolera les trois autres manières d'imposer une contrainte interne à la machine numérique, et se focalisera sur l'étude de ces prescriptions numériques.

III. L'apparition du réseau internet

On vit presque une époque de « Grandes Découvertes » tant les progrès technologiques réalisés entre les années 1980 et les années 2020 sont vertigineux. L'un des progrès les plus présents dans notre société contemporaine fut l'apparition du réseau numérique. Tout d'abord, comment définir le « réseau » ? Quel que soit le contexte dans lequel on le mobilise, le réseau est par excellence le concept qui brave les règles de séparation de la matière. Les lois de la physique ne rassemblent pas la matière dans un même corps uniforme, mais la morcèle en plusieurs entités éparses : les êtres humains sont physiquement éloignés les uns des autres, tout comme il existe une distance entre deux lampadaires ou, pour ce qui est de notre anatomie, entre le coeur et les reins. Or, chacun de ces fragments de matières remplit **une fonction, c'est-à-dire un problème qu'il doit résoudre**¹⁵. Le morcellement naturel de la matière empêche donc toute communication entre ces fonctions :

- (i) Isolés, les êtres humains ne peuvent partager leurs connaissances et déductions. Les connaissances et déductions remplissent notamment les fonctions d'identifier des erreurs et des solutions (connues ou déduites de connaissance), mais aussi d'en tirer de nouvelles questions à résoudre et de faire des découvertes en les résolvant. Si les connaissances et déductions des êtres humains sont isolées les unes des autres, si ces derniers ne les partagent pas entre eux, il est difficile de bâtir une société humaine sur le progrès.
- (ii) Les lampadaires au fonctionnement exclusivement individuel ne peuvent mutualiser ni coordonner leurs éclairages. Si cet isolement entre les lampadaires se maintient, il sera donc difficile (mais possible par allumage manuel) de se repérer la nuit en milieu urbain.
- (iii) Sans les artères ni les veines pour transporter le sang depuis le coeur, les reins ne seraient plus alimentés en sang. Si l'isolement entre le coeur et les reins se maintient, il est donc impossible pour un être humain de survivre.

S'affranchir de l'éclatement de la matière revêt donc une importance capitale, se montre parfois même nécessaire. Ici réside la fonction du réseau - l'affranchissement de la disjonction physique. **On définira alors le réseau comme un ensemble de liens permettant de s'affranchir des règles de séparation physique entre les choses ainsi reliées.** Il existe différents types de réseaux, qui peuvent se distinguer notamment selon leur objet (le « réseau universitaire » a l'université pour objet, le « réseau professionnel » a le travail pour objet, le « réseau neuronal » a pour objet les neurones...) ou encore selon leur moyen de réalisation (le « réseau urbain » se réalise au

¹⁵ Cette définition s'inspire de celle donnée par Niklas Luhmann à la « fonction », v. LUHMANN N., *Grundrechte als Institution. Ein Beitrag zur politischen Soziologie*, Dunker & Humblot, 2009 [publication originale en 1965]. Une chose peut remplir une fonction, soit parce qu'elle y est obligée, soit parce qu'elle s'y oblige elle-même. Par exemple, une chaise a notamment pour fonction de résoudre le problème suivant : « permettre à l'être humain de manger assis et à un niveau confortable par rapport au niveau de la table ». Ou encore, l'État s'oblige lui-même à résoudre des problèmes de conflits de lois (par des techniques comme des exceptions légales, le contrôle de proportionnalité, l'évincement d'une loi au nom de principes...), ce qui octroie notamment à l'État la fonction de résoudre de tels conflits. On retiendra la même définition pour les « fonctions logicielles », qui sont elles aussi chargées de résoudre des problèmes.

moyen de l'urbanisation, le « réseau ferroviaire » se réalise au moyen de rails, le « réseau électrique » se réalise au moyen de l'électricité...).¹⁶.

On s'intéresse ici au réseau internet, qui est lui-même un type de réseau électrique. Internet est le fruit d'une longue période de recherches et d'expérimentations entre la fin des années 1930 et 1970. En 1936, le mathématicien Alan Turing théorise la « machine de Turing » en essayant de définir le concept d'algorithme. Contrairement à ce que suggère son nom, la machine de Turing ne se présente pas sous la forme d'une machine mais d'une procédure mathématique. Cette « machine » est composée : d'un ruban infini constitué de cases (à l'image d'une pellicule de film que l'on pourrait dérouler sans fin) ; d'une personne virtuelle qui lit et écrit les symboles contenus dans chaque case du ruban ; d'un registre d'états qui recense un nombre fini d'états possibles ; et d'une table d'actions (ou « programme ») qui indique à la personne virtuelle le symbole qu'elle doit écrire sur le ruban. La procédure mathématique est la suivante : la personne virtuelle lit une case du ruban ; elle consulte le registre d'états pour connaître l'état qu'elle doit adopter en l'espèce ; enfin, elle consulte la table pour savoir le symbole à écrire dans la case. Par exemple, « si la personne virtuelle est dans l'état 39, et si le symbole contenu dans la case est 0, alors la personne virtuelle doit remplacer 0 en y écrivant 1 à la place, passer à l'état 27 puis lire la case adjacente à droite »¹⁷. Cette procédure mathématique est sensée pouvoir résoudre n'importe quel problème par le calcul.

En janvier 1940, Arthur H. Dickinson, employé d'IBM, conçoit le premier ordinateur numérique, i.e. la première machine capable d'encoder des informations en les faisant correspondre à des combinaisons de chiffres ¹⁸ . L'ordinateur de Dickinson encodait les informations d'après le système décimal (0 à 9) et, surtout, ne pouvait pas stocker de programme informatique. Il ne s'agissait donc pas encore d'une machine de Turing concrétisée, à défaut d'une table d'actions programmée dans la machine. Il faudra attendre mai 1941 pour qu'apparaisse la première machine de Turing, le premier ordinateur numérique programmable : le Z3, conçu par l'allemand Konrad Zuse. À la différence de l'ordinateur de Dickinson, le Z3 encode les informations d'après le système binaire (0 à 1) — c'est d'ailleurs le premier ordinateur numérique à le faire.

En 1948, Claude Shannon analyse l'encodage binaire dans sa « théorie mathématique de la communication de l'information » (abrégée « théorie de l'information ») ¹⁹ . Il soutient que toute information communiquée à autrui peut être réduite à une équiprobabilité entre deux issues (oui/non, positif/négatif etc.). Dès lors, toute information exprimée peut être mesurée par l'issue qu'elle a prise parmi les deux proposées : l'issue A (notée par le chiffre 0) ou l'issue B (notée par le chiffre 1). Chaque issue est appelée « bit » (*binary digit*).

On l'illustre avec la structure des « interruptions et exceptions » — un type d'instruction programmée nativement dans la machine pour les tâches les plus élémentaires comme « dessiner un pixel ». Une interruption est stockée dans la machine sous la forme d'un

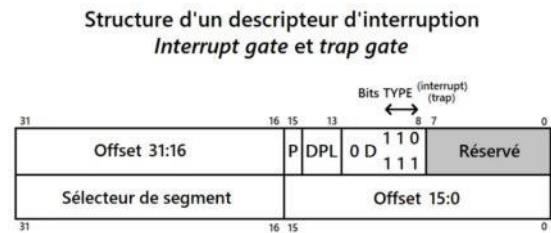
¹⁶ Pour d'autres exemples plus approfondis et originaux – réseau familial, réseau politique, réseaux artistiques tel le réseau moyenâgeux des cathédrales reposant sur les fleurs de lys sculptées et ornant les façades etc. –, v. notam. VERGER Jacques (dir.), *La forme des réseaux : France et Europe (Xe-XXe siècle)*, Actes des congrès nationaux des sociétés historiques et scientifiques, Editions du Comité des travaux historiques et scientifiques, 2017

¹⁷ On reprend cet exemple de la page Wikipédia consacrée à la machine de Turing

¹⁸ PUGH Emerson W., *Building IBM: Shaping and Industry and its Technology*, The MIT Press, 1995

¹⁹ SHANNON Claude, « A Mathematical Theory of Communication », *The Bell System Technical Journal*, vol. 27, juil-oct. 1948, p. 379-423, 623-656

« descripteur ». Dans un jeu d'instructions x86 (méthode de structuration des instructions développée par Intel en 1978), les descripteurs d'interruption/exception obéissent à la structure suivante ²⁰ : un champ offset de 32 bits et un sélecteur de segment de 16 bits qui, couplés, indiquent l'adresse de l'interruption, c'est-à-dire sa situation précise dans l'espace mémoire de la machine ; un bit de présence P, qui est fixé à 1 si l'interruption est présente dans la mémoire physique (*i.e.* la mémoire limitée par les capacités matérielles de la machine), ou qui est fixé à 1 si elle est absente de la mémoire physique (notamment si elle est présente en mémoire virtuelle, *i.e.* la mémoire augmentée par logiciel) ; deux bits DPL qui indiquent le niveau de privilège de l'instruction (00, 01, 10 ou 11 selon la zone plus ou moins privilégiée qu'occupe l'interruption dans la mémoire)²¹ ; un bit D qui indique la taille de l'entrée du descripteur (0 si le descripteur débute par 16 bits, 1 si l'entrée du descripteur s'étend sur 32 bits) ; trois bits TYPE qui indiquent le type de l'instruction (110 pour les *interrupt gate*, 111 pour les *trap gate*, 101 pour les *task gate*²²) ; enfin, huit bits « réservés » à d'autres programmes, qui sont donc définis par les programmes qui utilisent cette interruption.



Ce descripteur illustre la manière dont, en application de la théorie de Shannon, une suite de 0 et de 1 peut fournir des informations assez complètes à la machine pour lui permettre d'exécuter les données. L'information mesurée par bits est appelée « information numérique ». En 1949, le chef du groupe « Data Transmission » de la Division 2 du Laboratoire de recherche de Cambridge de l'Armée de l'Air des États-Unis, John Harrington, conçoit le premier modem capable de transmettre l'information par bits à une machine tierce (en convertissant les signaux analogiques en signaux binaires)²³. C'est la naissance du premier réseau numérique binaire. La même année, après que l'URSS a testé sa première bombe atomique en août, le Département américain de la Défense confie à un groupe d'études – surnommé le « Comité Valley » – la mission d'identifier les faiblesses de la défense aérienne des États-Unis. Le Comité constate que les stations de radars aux États-Unis ont une portée si limitée par leur horizon qu'ils ne peuvent pas détecter un bombardier ennemi avant que le bombardier détecte la station. Pour résoudre ce point faible, le Comité propose en 1950 d'installer des stations à proximité les unes des autres, donc d'en démultiplier le nombre. « Afin d'interpréter les signaux d'un grand nombre

²⁰ MIT Parallel & Distributed Operating Systems Group (PDOS), « Intel 80386 Reference Programmer's Manual Table of Contents », Chapter 9.5 IDT Descriptors, sur pdos.csail.mit.edu

²¹ Les niveaux de privilège divisent la mémoire en quatre niveaux qui évaluent la priorité avec laquelle des données stockées par la machine peuvent être exécutées par le processeur. Les données stockées au premier niveau (« noyau ») sont exécutées en priorité par le processeur ; celles stockées au quatrième et dernier niveau sont exécutées en dernière position. Le premier niveau s'écrit binairement 00, le deuxième niveau s'écrit 01, le troisième niveau 10 et le dernier niveau 11.

²² Les *task gate* ont un champ réservé à la place du champ offset, car ce type d'interruption représente généralement l'exception « double faute », seule exception à survenir sous l'effet d'une erreur qui la précède, *i.e.* à survenir exclusivement à cause d'un contexte d'exécution d'un programme. Précisément, l'exception double faute se produit lorsqu'entrent en conflit deux exceptions à exécuter simultanément, ce qui fait interrompre l'exécution de tout programme en cours voire met la machine hors tension (« écran bleu de la mort » de Windows etc.). Elle peut résulter d'un problème de ventilation, d'un excès de tâches, d'un problème de communication entre les composants de la machine etc.

²³ Laboratoire Lincoln du MIT, « SAGE: Semi-Automatic Ground Environment Air Defense System », sur ll.mit.edu [site web du Laboratoire Lincoln du Massachusetts Institute of Technology] ; Air Force Rocket Propulsion Laboratory, « March 22, 1987: Air Force Rocket Propulsion Laboratory Redesignated the Air Force Astronautics Laboratory », sur aftc.af.mil [site web du Air Force Test Center], 22 mars 2021

de radars, il fallait trouver un moyen de transmettre les données radar à un ordinateur central »²⁴. L'ordinateur pourrait ensuite « analyser les données en temps réel » et ainsi « détecter et intercepter l'avion hostile ». Il s'agit, à notre connaissance, du premier projet militaire consistant à interconnecter des terminaux (stations radar) avec un ordinateur, lesquels s'échangeraient des informations au moyen des lignes téléphoniques.

S'appuyant sur les conclusions du rapport du Comité Valley, le directeur des recherches scientifiques de l'Armée de l'air des États-Unis, Louis Ridenour, contacte à son tour le président du MIT fin 1950, James Killian. Le premier demande au second de rétablir un laboratoire dédié à la recherche sur la technologie radar après la disparition du Radiation Laboratory en 1949 (provisoire, censé ne pas s'étendre au-delà des circonstances de la seconde guerre mondiale). James Killian a d'abord refusé de participer à de nouveaux grands projets de guerre, mais Ridenour le convainc de restaurer ce laboratoire, sous le nom de « Projet Charles ». Le 20 avril 1951, les données émises par les radars ont été pour la première fois interceptées avec succès par un ordinateur via des lignes téléphoniques, détectant efficacement un faux avion ennemi. En août 1951, le rapport final du projet Charles conclut ainsi : « nous approuvons le concept d'un système centralisé tel que proposé par le Comité [Valley], et convenons que l'appareil central de coordination de ce système devrait être un ordinateur numérique électronique à grande vitesse ». Le rapport annonce la succession du Projet Charles par le Projet Lincoln, spécialisé dans la recherche de technologies militaires.

Dans le cadre de ses travaux, le Projet Lincoln étend le réseau de radars centralisé par un ordinateur, pour développer le **premier réseau d'ordinateurs** : au moyen de lignes téléphoniques et de modems, un vaste réseau connecte une foule de radars et de téléimprimeurs à plusieurs ordinateurs enfermés dans des bunkers militaires. Ce réseau SAGE (Semi-Automatic Ground Environment) est opérationnel en juin 1958.

Dans le cadre des travaux du MIT puis de l'ARPA (*Advanced Research Projects Agency*), une agence du Département américain de la Défense spécialisée dans la recherche de nouvelles technologies à des fins militaires, le psychologue Joseph Licklider contribue en 1962 à la création du projet MAC (*Multiple Access Computer*). Ce projet aspire à la création d'un ordinateur central capable de permettre la communication *concomitante* (là réside la différence avec les projets précédents) entre 30 usagers depuis leurs terminaux. À l'occasion du projet MAC, Licklider devient convaincu de l'intérêt d'un « partage, par les utilisateurs d'une même machine, de leurs programmes et de leurs données, de manière à ce que se constitue une base de connaissance et de savoir-faire dans laquelle tous les chercheurs pourraient piocher »²⁵. En 1964, Robert Taylor succède à Licklider, et revendique une meilleure collaboration entre chercheurs. Il confie à Larry Roberts, en 1967, la mission de réaliser le réseau décrit par Licklider. Taylor convainc le directeur de l'ARPA, Charles Herzfeld, de financer ce réseau, qui sera baptisé ARPANET. Dès 1968, ARPANET sera soumis à des appels d'offre, sonnant la fin du projet MAC. L'année suivante, ARPANET est expérimenté avec succès via les lignes téléphoniques de l'opérateur américain AT&T pour transmettre le message.

ARPANET fonctionnait de la façon suivante : à chaque poste était assorti un petit ordinateur IMP (*Interface Message Processor*). Chaque utilisateur peut produire des messages depuis sont

²⁴ « SAGE: Semi-Automatic Ground Environment Air Defense System », préc. sur *ll.mit.edu*

²⁵ BAMDÉ Aurélien, *L'architecture normative du réseau internet. Esquisse d'une théorie*, Thèse de droit, L'Harmattan, 2014, p. 36

poste. Pour transmettre un message à un poste destinataire, l'IMP local captait ledit message, l'acheminait vers l'IMP voisin, qui l'acheminait à son tour vers l'IMP voisin et ainsi de suite jusqu'à parvenir à l'IMP destinataire. L'IMP émetteur encapsulait les données (*i.e.* découpait les données en plusieurs paquets) et, pour alléger le travail du poste récepteur, l'IMP voisin du poste récepteur recompose le message (*i.e.* rassemble les paquets constitutifs du message)²⁶. ARPANET reposait donc sur un protocole de communication par commutation de paquets de poste-à-poste : le message découpé en paquets devait rebondir d'un poste au poste voisin pour atteindre le destinataire.

Les années 1970-80 ont vu éclore les réseaux numériques : en 1980, le réseau USENET est lancé, accessible à tous et utilisé comme « forum civil » mondial ; en 1981, BITNET et USENET sont créés pour relier les universités américaines ; et bien sûr, en juillet 1977, est mis à exécution le protocole TCP/IP, le protocole fondateur d'internet. Le TCP/IP est réalisé par l'interconnexion de trois réseaux en 1977 : ARPANET, SATNET (réseau satellite) et le réseau hertzien. En 1983, ARPANET abandonne officiellement son protocole de communication recourant aux IMP, et se rallie au protocole TCP/IP. Dans la suite des années 1980, les réseaux BITNET, CSNET et USENET s'interconnectent avec le TCP/IP. À la fin des années 1980, et surtout dans les années 1990, le réseau défini par le TCP/IP devient le Réseau des réseaux.

On décrira le fonctionnement d'internet plus loin dans la thèse, mais on peut commencer par exposer ici deux nouveautés apportées par le TCP/IP au regard d'ARPANET. Première nouveauté : bien que le TCP/IP reprenne la commutation par paquets, l'acheminement des paquets de données ne se fait plus de poste-à-poste, mais par le biais de routeurs. Au lieu de rebondir d'un poste au poste le plus proche du dernier emprunté, les données sont acheminées vers le routeur le plus proche de la destination, le plus disponible et/ou celui qui propose la route la plus sécurisée. Ce changement par rapport à ARPANET offre aux données d'atteindre rapidement une destination très éloignée, et ainsi de concevoir un réseau numérique à très grande échelle.

Deuxième nouveauté : les serveurs. Les serveurs ont pour fonction d'héberger des services (*i.e.* des logiciels comme des sites web, des jeux vidéo...) accessibles à distance par les utilisateurs. Cette accessibilité repose sur l'**environnement client/serveur** : l'utilisateur stocke sur sa machine des programmes appelés « clients » (navigateur web, application mobile...) qui comportent les instructions nécessaires pour communiquer avec les services hébergés sur les serveurs. Il n'est donc possible d'accéder à un service hébergé en ligne qu'à l'aide d'un client (accès à un site web depuis un navigateur web ou depuis une application mobile, accès à un jeu vidéo hébergé en ligne depuis un programme de jeu vidéo installé sur la machine de l'utilisateur...). Le client peut alors être défini comme le logiciel installé sur la machine de l'utilisateur depuis lequel cet utilisateur accède à un service

²⁶ Le découpage de données en paquets permet de supprimer les « bruits », c'est-à-dire les éléments parasites qui perturbent la communication. On l'illustre avec la communication téléphonique. La communication téléphonique était ininterrompue (du moins jusqu'à sa numérisation) : ne pouvant prédire le rythme de paroles d'une personne, le téléphone devait transmettre un débit constant pour que deux personnes communiquent sans interruption. Inversement, un message écrit diffusé sur un réseau numérique comporte des silences prévisibles entre chaque mot (par exemple, fictif, un espace entre chaque mot vaudra toujours 2 millisecondes). Ces silences gaspillent beaucoup de bande passante, *i.e.* la quantité maximale de données qui peut être transmise sur un réseau numérique. Leonard Kleinrock, Donald Davies et Paul Baran proposèrent alors que les données soient décomposées en paquets, supprimant ainsi les silences entre les données pour accélérer leur transmission sans surcharger le réseau de silences : v. *Ibid.* L'encapsulation des données permet aussi d'isoler ces dernières dans des paquets, préservant ainsi leur intégrité contre tout « bruit » parasite.

en ligne ²⁷ . Grâce à l'acheminement des données par des routeurs et à l'environnement client/serveur, le TCP/IP peut donc fournir un réseau à très grande échelle qui permet à ses utilisateurs d'accéder théoriquement à une infinité de services à distance.

On s'est permis de parler d'une période de « Grandes Découvertes » au regard des progrès technologiques effrénés depuis les années 1940. Ces progrès ont laissé voir des innovations spectaculaires depuis les années 1990, comme le Web en 1991, les réseaux sociaux depuis les années 2000, la technologie cloud, la blockchain, la cryptomonnaie et les objets connectés dans les années 2000-2010 et surtout, plus récemment, l'intelligence artificielle. On examinera dans cette thèse l'histoire et le fonctionnement de ces avancées ainsi que leurs enjeux et leurs relations avec la régulation juridique. L'intelligence artificielle (IA) n'occupera pas une grande place dans cette thèse, car notre objectif est d'abord de proposer une théorie de la régulation du réseau numérique. On constatera que les évolutions récentes et présagées de l'IA ne modifient pas la théorie qu'on proposera dans cette thèse.

IV. Les réseaux numériques, les rapports de force inter-humains et la régulation juridique

Compte tenu de l'échelle prise par internet, il n'est pas surprenant que ce réseau fit l'objet de très nombreux rapports de force. Par « rapports de force », on désigne la mise en rapport de plusieurs forces. Cette proposition appelle la définition de ce qu'est une « force », et l'identification du type de mise en rapport impliqué dans un rapport de force.

On appelle « force » une cause dont l'effet agit sur ce qui existe (sur une personne, un état mental, physique ou moral, une institution, un objet, une onde, une particule...). On insiste sur le fait que le terme *force* cible uniquement la cause elle-même et non son effet. Par exemple, la force physique de la pression a pour effet d'engendrer une contrainte (stress) sur la matière solide pressée ; la force économique de « l'offre de biens et services » a pour effet la production de biens et services, tout comme la force économique de la « demande de biens et services » a pour effet la consommation de biens et services.

²⁷ Par opposition à l'environnement client-serveur, les réseaux pair-à-pair (*peer-to-peer*, P2P) font de chacun de ses membre à la fois un client et un serveur. Dans un environnement client-serveur classique, plusieurs utilisateurs se connectent à un même serveur ou à un même groupe de serveur. Prenons l'exemple de Netflix : les serveurs exploités par Netflix hébergent les différents films et séries TV que l'entreprise propose à ses utilisateurs, et tous les utilisateurs doivent se connecter aux serveurs de Netflix pour accéder à son catalogue ; si le nombre d'utilisateurs et de requêtes est excessif par rapport aux capacités des serveurs de Netflix, ces derniers ne pourront pas répondre à toutes les requêtes, ce qui ralentira le trafic voire rendra Netflix inaccessible. Dans le cas du P2P, l'utilisateur doit d'abord installer un logiciel d'accès au réseau P2P qui partagera les ressources présentes sur le réseau entre chacun de ses membres. Par exemple, l'utilisateur d'un P2P peut soumettre un film que les autres utilisateurs pourront télécharger *sur l'ensemble du réseau*, c'est-à-dire en accédant à n'importe quelle autre machine utilisateur connectée au réseau P2P, car les fichiers constitutifs de ce film seront partagés entre les différents membres du réseau P2P qui jouent le rôle de serveur. Du fait de ce partage des ressources, une nuée de fichiers peut être partagée sans saturation du réseau. Le réseau P2P peut être entièrement décentralisé (hypothèse qu'on vient d'examiner) ou partiellement centralisé (si les utilisateurs doivent emprunter un serveur central pour communiquer entre eux).

Le rapport de forces est caractérisé lorsque la mise en rapport de deux forces au moins prend la forme d'un conflit, d'une contradiction entre ces forces²⁸. **Il y a rapport de force lorsque se contredisent deux forces qui agissent sur la même chose.** Dans ce cas, chaque force essaie plus ou moins de s'imposer à l'autre pour contrôler la chose qui fait l'objet du rapport de force. La force qui s'impose le plus « gagne » la bataille du contrôle ; celle qui cède le plus « perd » cette bataille²⁹.

En réalité, cette victoire apparente d'une force sur l'autre peut être destructrice pour la force « victorieuse ». Prenons l'exemple de l'équilibre hydrique, constitué par le ratio entrées/sorties de liquides dans l'organisme : si les forces qui provoquent les entrées de liquides s'imposent excessivement sur les forces qui provoquent les sorties de liquides, l'organisme subira une rétention de liquides ; si au contraire les forces qui provoquent les sorties de liquides s'imposent excessivement sur les forces qui provoquent les entrées de liquides, l'organisme subira une déshydratation. Si la rétention de liquides ou si la déshydratation est excessive, l'organisme meurt et aucune des deux forces n'a « gagné ». Le fait qu'une force s'impose excessivement à l'autre produit la destruction des deux forces dans l'organisme. De même pour l'équilibre acido-basique, c'est-à-dire le ratio acides/alcalins contenus dans l'organisme. Si les acides s'imposent excessivement sur les alcalins ou inversement, le fonctionnement cellulaire et enzymatique est entièrement perturbé et incapable d'assurer son rôle, engendrant à nouveau la mort de l'organisme³⁰.

Ce raisonnement est aussi valable pour les relations humaines. On l'illustre avec le cas d'une personne qui arnaque ses amis : l'arnaqueur obtient au total 2 000 euros de la part de ses amis ; se sentant floués, ses amis abandonnent l'arnaqueur ; interrogé sur les réseaux sociaux quant aux raisons de la fin de sa relation avec l'arnaqueur, l'un des amis publie une réponse qui fait part des malversations dont il a été victime ; le témoignage de cet ami sur les réseaux sociaux parvient à l'entourage professionnel de l'arnaqueur ; l'arnaqueur perd non seulement ses amis, mais peut aussi subir un harcèlement massif sur les réseaux sociaux et se faire licencier de son travail si sa réputation est entachée. L'arnaqueur a certes « gagné » 2 000 euros par la force de ses actions, mais il a perdu ses amis qui lui apportaient ce dont il avait besoin, ainsi que son travail, et sa réputation sur les réseaux sociaux. La victoire de l'arnaqueur a engendré la destruction d'une part importante de son existence personnelle. De la même manière que le rapport de force acides/alcalins a des conséquences sur d'autres rapports de force cellulaires et enzymatiques nécessaires à la survie de l'organisme, le rapport de force entre l'arnaqueur et ses

²⁸ Par exemple, le conflit entre le contrôle bureaucratique et la résistance des administrés : CROZIER Michel, « Administration et bureaucratie. Le problème des moyens organisationnels de développement », *Sociologie du travail*, 1962, p. 367-378. Le pouvoir s'établit ainsi dans le contexte d'une relation (CROZIER M., « Pouvoir et organisation », *Archives européennes de sociologie*, vol. 5, 1964, p. 52-64), de sorte que le pouvoir peut se définir comme « la capacité d'une personne A d'obtenir qu'une personne B fasse quelque chose qu'elle n'aurait pas fait sans l'intervention de A » (DAHL Robert, « The concept of power », *Behavioral Science*, n° 2, 1957, p. 201-215) : dans ce cas, s'opposent la force de contrôle de A et la force de résistance de B.

²⁹ Le sociologue Erhard Friedberg a ainsi défini le pouvoir comme la capacité à négocier en sa faveur un échange de comportements : FRIEDBERG E., *Le pouvoir et la Règle. Dynamiques de l'action organisée*, Seuil, 1993

³⁰ L'équilibre acido-basique est mesuré en pH par la concentration des particules cédées par les acides (ions H⁺). PAILLARD M., SRAER J.-D. Et ARDAILLOU R., « Rôle des cellules dans la régulation de l'équilibre acido-basique », *International Journal of Clinical and Laboratory Medicine*, vol. 25, 1970, p. 116-128 ; KOWALCHUK John M. et SCHEUERMANN Barry W., « Acid-Base Balance: Origin of Plasma [H⁺] During Exercise », *Canadian Journal of Applied Physiology*, sept. 1995 ; « Troubles de l'équilibre acido-basique », *Collège des Enseignants de Médecine Intensive Réanimation*, 2017

amis a des conséquences sur d'autres rapports de forces importants pour la survie sociale, professionnelle, économique voire physique de l'arnaqueur.

C'est pourquoi les forces ne se préservent pas en « dominant » un rapport de forces, en s'imposant excessivement sur les autres, mais en s'équilibrant suffisamment avec les forces contraires pour maintenir leur propre survie. La méthode de la régulation s'appuie très exactement sur ce constat. **La régulation consiste à équilibrer des forces contraires, en s'assurant qu'une force ne s'impose pas excessivement sur une autre ou qu'une force ne cède pas excessivement face à une autre, dans le but de préserver l'existence du système traversé par ces forces.** Ainsi, l'équilibre hydrique est régulé par diverses hormones comme l'hormone antidiurétique et l'aldostérone, garantissant que les entrées d'eau sont équivalentes aux sorties d'eau, et préservant de cette manière la survie de l'organisme³¹. De la même manière, l'équilibre acido-basique est auto-régulé par l'organisme, principalement grâce au rejet ventilatoire du dioxyde de carbone, aux reins et à certaines substances tampons comme les bicarbonates³². Si l'autorégulation fait défaut, il est toujours possible de recourir à une régulation extérieure pour rétablir l'équilibre perturbé et préserver la survie du système organique³³.

Par « régulation juridique » (ou juridico-étatique), on entend la régulation mise en oeuvre au moyen de normes juridiques. Cette thèse est consacrée à l'examen de la régulation juridique des rapports de force inter-humains qui se jouent dans le cyberspace. On a vu que l'expression « rapports de force » peut couvrir des rapports de force économiques, institutionnels, sociaux, professionnels, familiaux, religieux et même biologiques ou encore politiques. Que recouvre l'expression « rapport de force *inter-humains* » ? On a vu que tout rapport de force s'inscrit dans un contexte relationnel. On a vu aussi que le rapport de force s'exprime à travers les *effets* des forces contraires : aussi longtemps que les forces ne produisent pas d'effets, elles ne se contredisent pas, et ne donnent donc lieu à aucun rapport de force. Le rapport de force naît donc *concrètement* de la contradiction entre les effets de plusieurs forces en présence. On a vu par ailleurs que le rapport de force ne surgit que lorsqu'une force tente de s'imposer à une force contraire au moins. Enfin, on voit deux moyens principaux grâce auxquels des êtres humains peuvent tenter de s'imposer à d'autres : leurs actes (y compris les actes de parole, d'écriture, de mouvement, de présence...) ; et leurs décisions (d'édicter une loi, de transférer de l'argent, de rester silencieux...). On définira alors le rapport de force inter-humain comme (i) tout type de relation interindividuelle ou de groupe par laquelle (ii) des êtres humains (iii) imposent concrètement (iv) leurs actes et/ou décisions à d'autres êtres humains.

³¹ JÉQUIER Éric et CONSTANT Florence, « Pourquoi faut-il boire de l'eau ? Pour maintenir la balance hydrique », *Cahiers de Nutrition et de Diététique*, vol. 44, sept. 2009, p. 190-197

³² BRIVET François G. et JACOBS Frédéric M., « Anomalies de l'équilibre acido-basique d'origine métabolique », in OFFENSTADT Georges, JAEGER Albert, BOLLAERT Pierre-Édouard, SAULNIER Fabienne, WOLFF Michel et ZÉNI Fabrice (dir.), *Réanimation Médicale*, 2e édition, Elsevier Masson, 2009, p. 1350 : « le métabolisme cellulaire produit quotidiennement entre 15 000 et 20 000 mmol de CO₂, ce qui devrait entraîner une importante formation d'acide carbonique et d'ions H⁺ [i.e. de particules acides], mais le système respiratoire en éliminant en continu une quantité de CO₂ équivalente à la production journalière, maintient le pH constant (pH : 7,37-7,43) »

³³ Dictionnaire médical de l'Académie française de Médecine, Entrée « équilibre acido-basique » : « l'équation d'Henderson-Hasselbalch explique le mécanisme de [l'équilibre acido-basique] en fonction de la concentration en bicarbonates et de la [pression partielle en dioxyde de carbone dans le sang artériel, i.e. l'oxygénation du sang]. Elle permet de comprendre le jeu des compensations ventilatoires et rénales et d'ajuster le traitement pour rétablir un équilibre perturbé »

On aura l'occasion de faire plusieurs applications de cette définition dans la thèse. Certes, les rapports de force inter-humains qui ont pour objet *le réseau internet* se déclinent sous de nombreuses manifestations — batailles économiques pour le contrôle des technologies en réseau (rapports de forces inter-humains économiques), volontés politiques de maîtriser internet ou de le libérer de toute étatisation (rapports de force inter-humains politiques) etc. Cependant, les rapports de force inter-humains qui se jouent *dans le cyberspace* (i.e. dans l'espace mémoire interconnecté au moyen d'internet) résultent exclusivement de la production de données binaires qui contraignent la machine à stocker, dans ce grand espace mémoire, des données exécutables ou à y exécuter des données stockées. Pour réguler les rapports de force inter-humains qui se jouent dans le cyberspace, il nous semble donc nécessaire de s'intéresser aux contraintes internes que les êtres humains imposent aux machines lorsqu'ils produisent des données binaires. Dans le cas contraire, les rapports de force inter-humains qui se jouent dans le cyberspace seront régulés à partir de leurs conséquences, et non de leurs conditions de naissance.

En somme, on peut ainsi résumer les liens qu'on entrevoit entre le réseau internet, les rapports de force interhumains et la régulation juridique : les êtres humains contraignent les machines numériques à stocker et à exécuter des règles ; une fois ces règles exécutées par la machine, les êtres humains obtiennent un résultat informatique (consommation illicite d'oeuvres protégées, harcèlement en ligne, diffusion de fausses informations, diffusion de propos haineux, cyberattaque, arnaque en ligne, publication de photos sexuelles par un(e) ex-partenaire à des fins vindicatives...) ; les rapports de force inter-humains qui naissent de l'espace mémoire interconnecté par internet résultent des données produites et des résultats informatiques obtenus dans cet espace, donc des contraintes exercés par les êtres humains sur les machines numériques ; la régulation juridique de ces rapports de force passe donc par un contrôle de ce pouvoir de contrainte exercé par les êtres humains sur les machines numériques, sans lequel contrôle les êtres humains peuvent exercer ledit pouvoir de contrainte sans limite. On vérifiera si cette articulation est exacte à l'aide d'une méthodologie scientifique. On verra que le pouvoir de contrainte exercé par l'être humain sur la machine numérique est déjà largement soumis à diverses techniques de contrôle (blocage, filtrage, suppression de données...) mises en oeuvre sur le fondement de normes juridiques. Enfin, on se demandera si ces techniques sont efficaces, et comment elles peuvent l'être.

V. Méthodologie et problématique

Cette thèse privilégie la méthode comparative. On s'inspirera à ce titre d'un maître de la méthodologie comparative dans les sciences juridiques, Guillaume Tusseau. Sa thèse de doctorat³⁴ rappelle que toute comparaison entre concepts nécessite de recourir à un méta-concept qui les surplombe : comparées sous le méta-concept « légumes », une carotte et une pomme de terre présentent certains traits communs (leur pousse dans le sol, leur comestibilité...) et certaines différences (la pomme de terre est un féculent contrairement à la carotte, les conditions de cultivation divergent...) ; comparées sous le méta-concept de la couleur « orange », la carotte et la pomme de terre présenteront d'autres traits communs (sur le marché, la majorité des carottes et certaines variétés de pommes de terres sont oranges) et différences (sur le marché, certaines carottes et la majorité des pommes de terres ne sont pas oranges) ; comparées sous le méta-concept « chaise », elles ne présenteront en

³⁴ TUSSEAU Guillaume, *Les normes d'habilitation*, Dalloz, 2006, p. 255s.

principe aucun trait commun car ni la carotte ni la pomme de terre ne semble partage de caractéristique conceptuelle avec une chaise³⁵.

Le méta-concept a donc ceci d'utile scientifiquement qu'il permet de tirer des conclusions d'une comparaison entre concepts (les carottes et pommes de terre sont des légumes *donc* elles sont potentiellement comestibles, toutes les carottes et pommes de terre ne sont pas orange *donc* il existe probablement plusieurs variétés de carottes et de pommes de terre, les carottes et les pommes de terre n'ont pas de dénominateur commun manifeste avec la chaise *donc* elles n'entretiennent *a priori* qu'un faible rapport conceptuel avec ladite chaise etc.). De la même manière, cette thèse comparera sous le méta-concept de « prescriptions » la règle de droit avec la règle issue de productions de données binaires. Cette comparaison nous permettra d'en tirer plusieurs conclusions sur la spécificité des règles produites dans le cyberspace par rapport aux règles de droit.

Outre cette comparaison conceptuelle, notre travail tire ses conclusions de la comparaison entre sept ordres juridiques : la France ; l'Union européenne ; les États-Unis ; le Royaume-Uni ; la Russie ; la Chine ; et la Corée du Nord. Les quatre premiers ordres juridiques se situent à des endroits différents du spectre politique libéral, et on remarquera que ces différences se répercutent sur la structure de leur réseau internet national. Les trois derniers se situent à des endroits différents du spectre politique autoritaire, et on observera là aussi que la structure de leur réseau internet national se distingue très clairement entre ces trois pays. Cette mise en regard nous servira principalement à comparer l'efficacité des techniques de régulation employées, et les réactions des producteurs de données binaires face à ces techniques, afin d'en déduire des lois générales qui conditionnent l'efficacité d'une technique de régulation du cyberspace quel que soit l'ordre juridique concerné. La comparaison entre ces ordres juridiques offrira également l'occasion d'identifier les objectifs de régulation de ces différents pays, les attentes numériques différentes de leurs populations, et les techniques de contournement choisies par ces populations pour échapper aux techniques de régulation mises en oeuvre par l'État.

Les données sur lesquelles on s'appuie pour notre étude sont principalement extraites du corpus juridique (tel qu'on l'a défini) des ordres juridiques comparés, des documents fournis par les autorités compétentes, des chiffres et conclusions proposés par des études scientifiques et des articles de presse réputés fiables. Notre approche du cyberspace s'inspire en grande partie de la méthodologie systémique (théorie des systèmes), c'est-à-dire conçoit cet espace comme un ensemble organisé par les échanges qu'entretiennent ses composantes (les données binaires produites) entre elles et avec l'environnement extérieur au cyberspace (les dommages subis par les êtres humains).

Pour terminer sur le cadre méthodologique, cette thèse ne sera pas assez longue pour nous permettre d'analyser tous les outils exploitables par les rapports de force inter-humains qui se jouent dans le cyberspace (ci-après « rapports de force inter-humains en ligne »). On identifie deux outils exploitables par ces rapports de force : l'échelle de diffusion d'une donnée ou d'un ensemble de données (par exemple le nombre de machines qui stockent ou produisent des propos haineux) ; et le caractère plus ou moins critique d'une machine contrainte par une production de données binaires (par exemple un opérateur d'importance vitale dont les machines sont attaquées par un logiciel malveillant). Le premier outil détermine l'étendue d'une contrainte imposée par l'être humain

³⁵ Sur l'exemple de la pomme de terre et de la carotte, v. TUSSEAU G., « Sur le métalangage du comparatiste », *Revus*, n° 21, 2013 [en ligne sur journals.openedition.org]

aux machines connectées à internet ; le second détermine la gravité d'une telle contrainte en fonction de l'importance des machines contraintes. On s'intéressera ici uniquement au contrôle de l'échelle de diffusion d'une donnée sur internet.

Nous tenterons donc à travers ces pages de répondre à la problématique suivante : comment les normes juridiques peuvent-elles fournir un contrôle efficace sur l'échelle de diffusion d'une donnée dans le cyberspace, de façon à réguler juridiquement les rapports de force inter-humains en ligne ?

Pour y répondre, on consacre une Première Partie à l'étude des rapports de force inter-humains en ligne. Cette partie passe en revue les approches étatiques et scientifiques de ces rapports de force, et souligne l'influence des travaux scientifiques sur les stratégies juridiques mises en oeuvre par les États pour réguler ces rapports de force. On questionnera à ce titre la pertinence de la théorie aujourd'hui dominante (*Code is Law*) qui prête aux seuls programmeurs le pouvoir de contraindre la compréhension machinale et les actions en ligne. On opposera à ces diverses explications notre théorie des prescriptions numériques, qui reconnaît à tout producteur de données binaires - y compris les utilisateurs - le pouvoir de contraindre les actions des uns et des autres dans le cyberspace. Seront identifiées les différentes catégories de prescripteurs numériques en ligne, les six catégories d'êtres humains capables de contraindre les machines connectées à internet en produisant des données binaires, ces six catégories qui « font la loi » dans le cyberspace. Nous examinerons en détail les prescriptions numériques qu'ils produisent, ces règles qui n'existent que dans le cyberspace, et compareront le mode prescriptif numérique avec le mode prescriptif juridique en mettant en regard les conditions de production, d'exécution et d'ordonnancement des prescriptions numériques avec celles des prescriptions juridiques. On en déduira enfin que l'existence d'un mode prescriptif numérique propre donne lieu à ce qu'on appelle une « réalité prescriptive » incarnée par le cyberspace. On appelle « réalité prescriptive » tout système gouverné par ses propres modalités de production, d'exécution et d'ordonnancement des prescriptions, et doté d'un espace dans lequel ces prescriptions obéissent *exactement* à ce mode prescriptif et en-dehors duquel elles n'y obéissent plus exactement - à l'image de la réalité prescriptive juridique incarnée par l'État et ses habilités³⁶.

Dans une Deuxième Partie, nous n'examinerons plus la théorisation des rapports de force inter-humains en ligne mais leur régulation. Après avoir précisément défini le concept de régulation juridique, on verra comment l'appliquer au réseau internet. On distinguera deux

³⁶ Tous les États forment une même réalité prescriptive étatique par leurs points communs dans l'espace où s'expriment leurs prescriptions (un territoire délimité composé par une population), et dans les modes de production, d'exécution et d'ordonnancement des normes juridiques (un gouvernement ou un équivalent pour produire le droit, un système d'exécution des normes, et des interactions entre les normes existantes pour préserver la cohérence et le dynamisme de l'ordre juridique). Cependant, passés ces points communs, chaque État (France, Royaume-Uni, Espagne...) incarne sa propre réalité prescriptive, c'est-à-dire possède ses propres conditions de production et d'exécution des normes et son propre espace territorial, de sorte qu'une règle exécutable dans un État ne le sera pas de la même façon dans un autre, voire ne le sera pas du tout. Ainsi, une réalité prescriptive n'est formée que par les points communs que partagent ses prescriptions à travers leur espace de déploiement et leurs conditions de production, d'exécution et d'ordonnancement. Il existe une réalité prescriptive étatique « générale » (définie par le droit international et la théorie du droit), tout comme il existe des réalités prescriptives particulières à chaque État ; une réalité prescriptive fédérale « générale » (points communs généraux des Fédérations) et des réalités prescriptives fédérales particulières à chaque Fédération ; une réalité prescriptive générale des villes et des réalités prescriptives particulières à chaque ville etc. En appliquant notre définition, on n'hésitera pas non plus à qualifier l'Union européenne de réalité prescriptive.

types de techniques de régulation : celles qui restreignent l'accès à des données dont le régulateur souhaite réduire l'échelle de diffusion (techniques de restriction de l'accès) ; et celles qui augmentent l'accès à des données dont le régulateur souhaite amplifier l'échelle de diffusion (techniques d'augmentation de l'accès). Seront analysées huit techniques de restriction de l'accès : (i) la coupure de l'accès à internet ; (ii) la suppression de données ; (iii) le chiffrement ; (iv) l'avertissement précédant l'accès à certaines données ; (v) le ralentissement de l'accès ; (vi) le blocage de l'accès ; (vii) le filtrage de l'accès ; et (viii) la centralisation. Cette analyse sera complétée par celle de sept techniques d'augmentation de l'accès : (i) la décentralisation ; (ii) le raccordement de l'accès à internet ; (iii) l'accélération de l'accès ; (iv) la redirection de l'accès ; (v) la création et la pluralisation de données ; (vi) la surexposition de données (notamment au moyen d'algorithmes) ; (vii) la réutilisabilité des données. Les techniques rapportées ne le sont pas exhaustivement, mais elles offrent un échantillon qu'on estime suffisant pour expérimenter leur efficacité dans chacun des sept ordres juridiques comparés. On listera les avantages et inconvénients de ces techniques, ainsi que les cas dans lesquels les États ont réussi à maximiser leurs avantages ou ont aggravé leurs inconvénients, d'où on déduira les situations auxquelles elles sont adaptées ou inadaptées. Les techniques d'augmentation souffrent principalement du risque d'être délaissées par les prescripteurs numériques en ligne, tandis que les techniques de restriction souffrent du risque d'être contournées. On recensera quatre configurations de contournement, qui nuisent à l'efficacité des techniques de restriction : la migration ; la feinte ; le saut ; et l'affranchissement. Pour conclure cette Deuxième Partie, on proposera une théorie en principe valable pour tout ordre juridique, destinée à évaluer et à réduire les risques de délaissement et de contournement, et ainsi contrôler efficacement l'échelle de diffusion d'une donnée grâce aux techniques de restriction et d'augmentation adaptées aux circonstances.

PREMIÈRE PARTIE – L'ÉTUDE DES RAPPORTS DE FORCE INTERHUMAINS EN LIGNE

Les chercheurs en sciences sociales ont très tôt tenté de comprendre les causes, les modalités et les implications des rapports de force exercés sur le réseau internet. Depuis les années 1990, ce « *Far West de la communication* »³⁷, cette « *conquête de l'Ouest* »³⁸ en ligne fascinent, entre autres pour les défis auxquels ils soumettent l'État et sa souveraineté³⁹. À cette époque, les États libéraux concevaient peu à quel point ce réseau pourrait être dommageable pour l'efficacité de leurs ordres juridiques respectifs.

Certaines bases juridiques devaient être posées pour déjouer les inefficacités prévisibles et prédites par le discours scientifique. Devaient être : harmonisées les législations sur les règles de compétences en cas de litige international ; installée une coopération entre États contre les infractions les plus mondialement répandues et préjudiciables (pédo-criminalité en ligne, violations de droits d'auteur, cyberattaques...) ; régulés à une échelle régionale le commerce en ligne et ses risques (atteintes aux données personnelles, *spams*, publicités mensongères...) ; régis les pouvoirs, activités et obligations des fournisseurs d'accès à internet (FAI, ou « fournisseurs de services de communications électroniques »)⁴⁰. Ces conseils dispensés par les chercheurs ont trouvé un écho dans le droit positif étatique et interétatique dès la fin des années 1990 et le début des années 2000.

C'est toutefois au début de la décennie 2010 que le discours scientifique, renouvelé, intensifie son influence auprès de l'État. L'intérêt revivifié de l'État pour ce réseau est largement imputable à l'amplification du phénomène internet et des pouvoirs qu'il confère. Des oligopoles stables et incontournables émergent (Alphabet propriétaire des produits Google, Meta, Amazon...), des révolutions arabes sont puissamment stimulées et organisées sur des réseaux sociaux que la Tunisie, l'Égypte et la Syrie sont alors incapables de juguler⁴¹, des abus de la liberté d'expression (propos haineux, harcèlement, injures...) prospèrent dans l'espace public comme des flux indomptables de données⁴², des cyberattaques et autres technologies militaires sont utilisées comme armes de guerre par des États contre d'autres États⁴³ (Russie contre Estonie en 2007, StuxNet en 2010, Flame en 2012...). Internet révèle son potentiel d'assaut contre les ordres

³⁷ WOLTON Dominique (sociologue), *Penser la communication*, Flammarion, 1997, p. 248

³⁸ CRUMLISH Christian (informaticien), *The ABC's of the Internet*, Sybex, 1996, p. 125

³⁹ PERRITT Henry H. Jr (juriste), « Cyberspace and State Sovereignty », *Journal of International Legal Studies*, vol. 3, 1997, p. 155-204

⁴⁰ Sur ces mises en garde, v. HARDY Trotter, « The Proper Legal Regime for "Cyberspace", *University of Pittsburgh Law Review*, vol. 55, 1994, p. 993-1055 ; WU Timothy, « Cyberspace Sovereignty ? The Internet and the International System », *Harvard Journal of Law and Technology*, vol. 10, 1997, p. 647-666

⁴¹ DICKINSON Rob, « Transformation of the Modern State: States Sovereignty and Human Rights in the Internet Age », *Connecticut Journal of International Law*, vol. 29, 2013, p. 51-68

⁴² PHILLIPS Whitney, « LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online », *First Monday* [en ligne], vol. 16, 2011

⁴³ Dès 2007, l'ingénieur Daniel Ventre recense diverses technologisations militaires sur trois continents et y applique le terme de « guerre » pour les moderniser sous la forme de « cyberguerre » en 2010 (VENTRE Daniel, *La guerre de l'information*, Paris, Lavoisier, 2007 ; *Cyberguerre et guerre de l'information*, Paris, Lavoisier, 2010). Aux États-Unis, c'est particulièrement l'avocat Harold Hongju Koh qui, après un discours remarqué le 18 septembre 2012 à l'Université de Harvard, a influencé la doctrine militaire américaine en appelant de ses vœux un « droit de la guerre » pour le cyberspace (HONGJU KOH Harold, « International Law in Cyberspace » [en ligne], *Harvard International Law Review*, vol. 54, 2012).

juridiques, et certains chercheurs pointent déjà les menaces que ce réseau réfléchit sur l'autonomie politique voire constitutionnelle des États en redéfinissant les équilibres démocratiques dans le monde entier⁴⁴. La violence, qui n'était plus négligeable, avec laquelle les États ont été frappés par internet a interpellé leur vigilance et fortement orienté leur attention vers les travaux conduits pour démêler les rapports de force en ligne et en détecter les règles. Il sera ainsi question, dans un premier temps, d'examiner la réception qui a été faite en droit positif des théories dégagées pour clarifier ces rapports de force en ligne (**Sous-Partie 1**).

Cependant, si ces théories ont souvent retenu le réseau ou ses acteurs comme échelle d'investigation, rares sont celles qui ont considéré la « donnée en ligne » comme unité de mesure des rapports de force sur internet. À cette nano-échelle, chaque donnée agit telle une prescription : pour la machine membre du réseau (ordinateur, smartphone, serveur, routeur, objet connecté...), la donnée produite par un utilisateur ou un programmeur ne représente rien d'autre qu'un ordre d'exécuter une règle ou de stocker une règle exécutable. Le réseau internet forme ainsi un conglomerat de prescriptions qui, sous les traits de « données binaires », commandent leur exécutabilité ou leur exécution. On verra alors dans un deuxième temps la manière dont les productions de données binaires, contraignantes pour la machine, provoquent les rapports de force inter humains qui se jouent dans le cyberspace (**Sous-Partie 2**).

Sous-Partie 1. L'identification des rapports de force en ligne par les États et chercheurs

L'étude d'internet et de son caractère régulable reposent sur de constructions scientifiques enrichies depuis les années 1990. Ces constructions sont fondées sur deux angles de vue : l'un observant internet de l'extérieur, comme un outil appelant régulation nonobstant ses spécificités indiscutables ; l'autre posant son regard sur l'« intérieur » du réseau internet, comme si le réseau abritait une société qui ne répondait que de ses propres règles.

Ces prises de positions peuvent paraître contradictoires, à plus forte raison quand la deuxième école percevait l'autonomie et l'autogestion d'un « cyberspace », tandis que la première école niait l'existence même d'un cyber espace, opposant que le réseau n'a rien de magique et dépend toujours d'une matérialité maîtrisable. Pour autant, cette opposition renvoie à une différence de points d'observations vis-à-vis d'internet, plus qu'à une contradiction⁴⁵. On verra que ces éclairages intérieur/extérieur d'internet sont complémentaires pour explorer les jeux de pouvoir en ligne de façon panoramique.

⁴⁴ TÜRK Pauline, « La souveraineté des États à l'épreuve d'internet », *Revue du droit public et de la science politique en France et à l'Étranger*, n° 6, 2013, p. 1489s.

⁴⁵ On songe ici à l'image du belvédère reprise par Michel Miaille de Michael Löwy dans *Paysages de la vérité* (1985), rappelant que l'esprit critique ne consiste pas à invalider un point de vue par sa contestation mais à considérer sa provenance selon une certaine hauteur, par définition variable selon celle à laquelle se place l'observateur (MIAILLE Michel, « La critique du droit », *Droit et Société*, n° 20/21, 1992, p. 80). L'analyse critique d'un objet repose sur une pluralité d'explications valides selon la hauteur depuis laquelle elles sont émises. Par exemple, les règles qui régissent une montagne ne peuvent être saisies que si, depuis l'extérieur, est étudié son ubac autant que son adret et si, depuis l'intérieur, sont examinés les étages qui la composent et les lois géologiques sans qu'aucune de ces explications ne se contredise mutuellement. C'est la mise en lumière de l'objet sous plusieurs éclairages qui permet de connaître complètement cet objet.

La première construction correspond à ce qu'on appellera « conception exogène d'internet ». Sa grille de lecture détache le réseau machinal de son acteur humain : l'être humain est extérieur à internet, il ne fait qu'*utiliser* une technologie avec toutes les originalités qu'elle recèle. Les rapports de force en ligne sont étudiés par le prisme de la personne humaine, soit qu'elle exerce un pouvoir sur le réseau (intervention extérieure sur le réseau), soit qu'elle subit un tel pouvoir depuis le réseau (effets externes du réseau). (**Chapitre 1**)

La deuxième construction correspond à ce qu'on appellera « conception endogène d'internet ». Elle tient le réseau et ses acteurs pour fusionnels : les actions pratiquées sur internet n'existent pas en-dehors de ce réseau, si bien que les acteurs d'internet sont distincts des acteurs urbains par leurs actions. Les rapports de force en ligne sont ici examinées à partir d'acteurs et d'actions propres et internes au réseau (**Chapitre 2**).

Chapitre 1. La conception exogène du réseau internet

La conception exogène place une distance entre le réseau et ses acteurs, distance qui peut être attribuée soit à la machine faisant écran entre l'acteur et le réseau, soit à la nature humaine de l'acteur qui le distingue de la nature numérique du réseau. Cette divergence a cultivé deux axes d'analyse, souvent complémentaires. Le premier qu'on baptisera « hardwariste » identifie les sources du pouvoir en ligne dans le fonctionnement technique du réseau internet (**Section 1**). Le second, qu'on dira « social », les identifie au contraire dans les usages socio-pragmatiques d'internet (**Section 2**).

Section 1. La distanciation du réseau et de ses acteurs par la machine selon l'axe hardwariste

Pour comprendre le point de vue technique sur laquelle repose cet axe (Paragraphe 2), encore faut-il cerner le fonctionnement technique du réseau internet (Paragraphe 1).

Paragraphe 1. Le fonctionnement du réseau internet

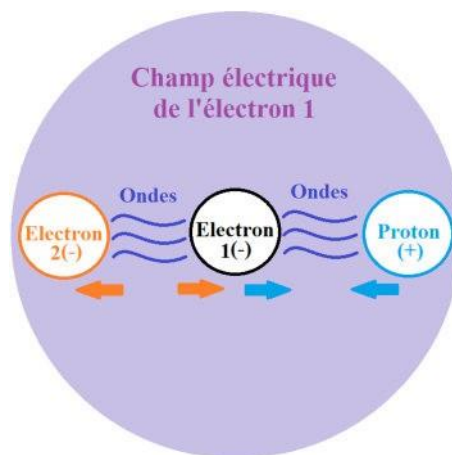
La compréhension technique des réseaux électriques (A) et numériques (B) offre non seulement la compréhension du réseau internet mais surtout l'isolement de son étude (C).

A) Le réseau électrique en toute technicité

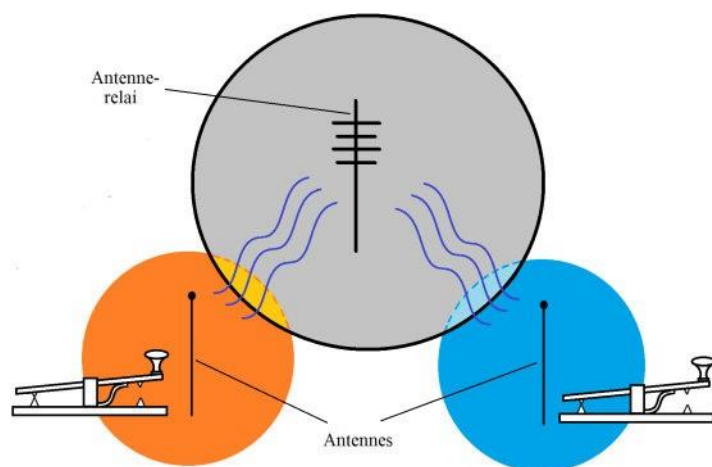
Pour rappel, un « réseau » a été défini en introduction comme **un ensemble de liens permettant de s'affranchir des règles de séparation entre les choses ainsi reliées**. Le réseau électrique, qui nous intéresse ici, se réalise au moyen de l'électricité. Plus exactement, ce qui brise la règle de séparation des choses, ce qui fabrique un lien entre ces choses devenues membres d'un tel réseau, c'est le courant électrique.

Les réseaux électriques font leurs débuts industriels, puis administratifs, commerciaux et domestiques dans la deuxième moitié du XIXe siècle. La liaison est d'abord filaire : les membres du réseau (encore appelés « points » ou « noeuds ») sont reliés *par des câbles* qui transportent le courant électrique. À la fin du XIXe siècle, Heinrich Hertz découvre que le courant électrique peut être transporté *par les airs*, sans nécessiter de câbles pour relier les points du réseau. En fait, il démontre que deux charges électriques (électrons, neutrons, protons) peuvent communiquer à distance, sans le moindre contact physique.

Depuis la loi de Coulomb de 1785, il est connu des physiciens que toute charge électrique génère un champ électrique autour d'elle. Ce champ s'étendra si l'intensité de la charge électrique est augmentée (par ex. en amplifiant le courant électrique sur l'éclairage d'une ampoule), et il rétrécira si l'alimentation électrique de la charge est diminuée (par ex. en éteignant l'ampoule). Si une charge se situe dans le champ électrique d'une autre charge, les deux interagissent soit en se repoussant si elles sont de même signe (positif ou négatif), soit en s'attirant si elles sont de signe contraire. Une *force à distance* s'exerce donc d'une charge à l'autre, et cette force s'exerce par le biais d'« ondes électromagnétiques ». L'onde étant l'antonyme de la matière en physique classique, il y a donc bien ici une communication immatérielle entre les charges.



Les ondes électromagnétiques peuvent être visibles (c'est le cas de la lumière naturelle qui permet de voir les couleurs et dont la vitesse correspond à celle de ses ondes) ou invisibles. C'est à Hertz que l'on doit la découverte de celles invisibles. L'enjeu industriel s'est vite déclaré : si une charge qui reçoit un signal électrique peut le transmettre à distance à une autre charge, alors il suffit de confectionner un support qui recevra des charges électriques puis les communiquera par les airs à un support destinataire.



Ainsi a surgi la télégraphie sans fil (TSF ou radiotélégraphie) dès 1901. Empruntant d'emblée le système proposé par Samuel Morse qui avait déjà fait relier par câbles ses manipulateurs dans la deuxième moitié du XIXe, les radiotélégraphistes appuyaient sur le levier du manipulateur Morse pour le faire taper contre un interrupteur situé en-deçà. Relié par câbles à des machines génératrices de courant

électrique (alternateurs à haute fréquence, lampes à vide...), cet interrupteur produit des charges électriques à chaque pression qui, selon la durée et le rythme des impulsions, correspondent à des messages codés par des points (signal bref) ou des traits (signal durable). Seulement, pour que le message émis parvienne à son destinataire, encore faut-il que l'émetteur et le récepteur se situent dans le même champ électromagnétique. C'est là le rôle des antennes électriques, abondamment chargées pour que leur champ électromagnétique s'étende le plus loin possible⁴⁶. Pour être expédié puis réceptionné, le télégraphe devait alors traverser l'antenne ou les antennes électriques du réseau hertzien ainsi institué.

Le format télégraphique était toutefois alourdi par au moins deux handicaps conséquents. Sa traduction, d'une part, ralentissait la compréhension du message voire compromettait les

⁴⁶Dans la limite ce qui est humainement supportable (trop chargées, les ondes électromagnétiques se muent en rayons X, Y voire Z particulièrement nocifs pour la santé humaine)

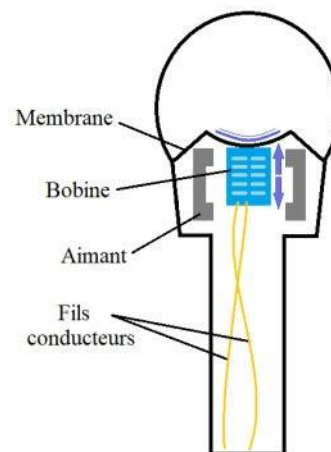
communications urgentes et, d'autre part, requérait une telle maîtrise du code employé que l'usage en était réservé à quelques-uns. Le défi technique à relever résidait à présent dans le dépassement des messages codés (donc le dépassement de la télégraphie) par la transmission aérienne de messages « bruts », exempts de tout chiffrement. L'objectif est atteint avec l'apparition de la radiophonie dans les années 1910. Le réseau hertzien devient capable de faire circuler du son et la première station radio régulière, TSF, voit le jour en 1914.

Ce passage du télégraphique au phonique dans la radiodiffusion n'allait pas de soi. Rappelons à cet égard que, le réseau hertzien n'étant pas humain, il n'en comprend pas le langage mais réagit aux seuls signaux électriques et à rien d'autre : il ne transporte pas des pastèques mais des charges électriques. Inversement, la signification des signaux électriques n'est pas très accessible à l'entendement humain. Ce que transporte le réseau hertzien n'est donc compréhensible pour l'être humain qu'après une conversion en deux temps. *Primo*, les charges électriques doivent être ramenées à une unité de mesure cohérente (par ex., le système du Morse convertit les charges en symboles « points-traits »). *Secundo*, cette unité de mesure doit coïncider avec un langage humainement intelligible (par ex. le système du Morse fait coïncider les symboles aux lettres de l'alphabet). Autant le système du Morse est aisément mesurable car sécable – *tel* nombre de charges sur *telle* durée était impulsé coup sur coup. Autant, il est bien moins commode de quantifier un son continu, oscillant et tonal – comment le mesurer, et comment rendre sa mesure intelligible à l'être humain ? La méthode analogique en apporta les réponses en respectant les deux temps de la conversion. *Primo*, cette méthode fait concorder un élément dont on cherche la reproduction (« élément capté » comme le son) avec une grandeur analogue mesurée le plus fidèlement possible. *Secundo*, la mesure de cet élément et de ses variations est rendue intelligible pour l'être humain grâce à un outil appelé « transducteur ». À la température (élément capté) correspondent des degrés Celsius, Kelvin ou Fahrenheit (grandeurs analogues) dont la mesure est reproduite par un thermomètre (transducteur) ; au temps correspondent des secondes, minutes ou heures dont la mesure est reproduite par une montre etc.

Appliquée au son et au réseau hertzien, cette méthode s'attèle à mesurer non les tonalités « acoustiques » d'un son⁴⁷ mais ses tonalités « électriques ». En effet, si le réseau hertzien peut transporter du son, c'est parce qu'un son est *composé* de charges électriques. En reproduire les charges électriques aura donc pour effet de reproduire, de *recomposer* le son. Pour ce faire, Alexander Graham Bell s'en remet à une loi physique déjà établie et testée par H. Hertz : de ce que la charge électrique exerce une force à distance, il s'en déduit que les signaux électriques génèrent de légers mouvements aériens. Le son ne fait pas exception, et A. G. Bell se donne pour mission de capter ces remuements électromagnétiques aériens générés par le son afin d'identifier les charges électriques qui y correspondent. Le transducteur ouvré à ce titre est le microphone.

47Les tonalités acoustiques pourront d'ailleurs être mesurées à partir de 1923 avec la découverte analogique des décibels par Alexander Graham Bell. V. notam. l'émission « Comment appréhender l'unité de mesure du son, le décibel ? » de Michel Alberganti pour France Culture du 13 janv. 2012 [en ligne sur le site de France Culture]

Un microphone comporte une bobine solidaire d'une membrane et cernée par un aimant. Le mouvement aérien produit par le son fera vibrer la membrane et, avec elle, la bobine ; naturellement doté d'un large champ électromagnétique, l'aimant réagira aux ondes électromagnétiques qui se dégagent du son émis, ce qui amplifiera l'agitation de la bobine et en corrigera le battement conformément aux charges électriques reçues. La bobine se lèvera puis se rabattra alternativement au rythme du signal électrique impulsé et selon l'ampleur du mouvement aérien donné : elle reproduira, recomposera les caractéristiques des ondes ⁴⁸ ainsi captées. Au contact du champ électromagnétique de l'aimant, la cadence de la bobine génère un courant électrique qui imite les propriétés du son extérieur, et ce courant électrique sera transporté par des fils conducteurs auxquels la bobine est reliée. Une fois le son reproduit dans ses attributs électromagnétiques, il pourra véhiculer aussi bien sur un réseau filaire *via* des câbles que sur un réseau hertzien *via* des antennes électriques (stations de transmission de base pour la 1G, antennes-relais pour la 2G et les générations suivantes) et des supports émetteurs/récepteurs des charges électriques véhiculés (le téléphone, le poste de radio, le *talkie-walkie*, la chaîne Hi-fi...). Ainsi A. G. Bell, dont il n'est pas surprenant qu'il soit l'inventeur du téléphone, étend-il à toute la société un réseau sans fil jusqu'alors exploitable par les seuls radiotélégraphistes.



Ces précisions techniques sur le réseau électrique nous permettent d'en inférer une définition conforme à son fonctionnement : **par « réseau électrique », on désignera un réseau⁴⁹ qui relie des supports d'émission/réception** (manipulateur Morse, téléphone, poste de télévision...) **au moyen d'un courant électrique transmettant des signaux par voie filaire** (câbles souterrains, encastrés, sous-marins, fibre...) **et/ou par voie hertzienne** (antennes-relais, satellites pour les transmissions longue distance lorsque les antennes-relais sont insuffisantes, bornes wifi conçues en 1993 pour courte distance, bluetooth conçu en 1994 pour très courte distance...). Internet s'inscrit adéquatement dans la continuité de ces acquis technologiques puisqu'il emprunte un réseau électrique. Mais surtout, ces précisions donnent l'opportunité d'isoler notre premier objet d'étude, le réseau internet, afin de discerner dans son fonctionnement ce qui lui est spécifiquement imputable de ce qui est imputable au réseau électrique en général.

B) Le réseau numérique, créateur d'une nouvelle réalité

Au plan technique, le numérique représente surtout une révolution par rapport à l'analogique. Comme on l'a vu, l'analogique procède par reproduction analogue, c'est-à-dire en répliquant le plus identiquement possible l'élément capté. Paradoxalement, cette réplification était *trop* identique : lorsqu'un microphone captait les sons, il captait tous les sons dont le signal électrique intégrait le champ électromagnétique du micro. La voix était alors couverte par des sons indésirables (voix externes, souffle du vent...) autant que par des bruits de fond perturbateurs. Ces bruits de fond perturbateurs résultent des charges électriques qui composent l'environnement de l'utilisateur du microphone. En interagissant *via* leurs ondes et champs

⁴⁸À savoir leur fréquence (nombre de fois que le phénomène d'onde se produit en une seconde), leur vitesse (celle avec laquelle elles se diffusent dans l'espace) et leur longueur (l'interstice qui sépare deux maxima d'une onde retranscrite sous forme de courbe)

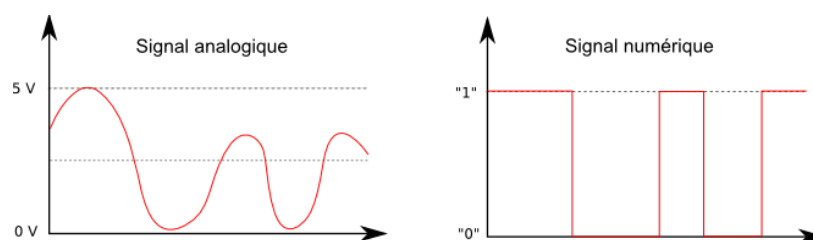
⁴⁹Tel que défini plus haut.

électromagnétiques, ces charges produisent des mouvements aériens invisibles pour l'Homme mais potentiellement parasites pour la captation microphonique si elles sont intenses.

Ce parasitisme ne sabote pas seulement la captation du signal. Il sabote jusque dans son transit, soit tout le fonctionnement du réseau hertzien, lui-même analogique : il n'était pas rare que le signal, relayé d'antenne en antenne pour atteindre son point d'arrivée, traverse des espaces du monde où la puissance de champs électromagnétiques perturbait la retransmission voire déviait carrément le signal. Ces défauts devinrent notoires à l'occasion des activités militaro-aériennes, explosions, essais nucléaires et bombardements précipités par la Seconde Guerre Mondiale. C'est là que s'intercale le paradoxe : tenant le rôle de biais naturels, les charges électriques et les ondes qu'elles émettent représentent une limite intrinsèque à l'analogique qui empêche d'isoler une composante (la voix) de l'élément capté (le son).

L'apport du numérique a été de franchir cette limite. Le numérique se consacre non à la reproduction d'un élément capté mais à sa *transformation*. Autrement dit, l'élément ne sera pas reproduit *en sa forme* ; lui sera plutôt *prêtée une forme* spéciale, numérique. Ce format numérique se présente comme une série de 0 et de 1, attendu que le 0 correspond à un signal négatif et le 1, à un signal positif. Les 0 et les 1, soit les « bits », portent des informations (v. Introduction). En restant sur l'exemple de la voix, imaginons que le mi bémol le plus grave corresponde aux bits 00000011 ; chaque fois que sera produite cette suite binaire, elle portera donc l'information que le mi bémol le plus grave est produit. Cela revient à dire que, à l'issue de cette suite 00000011 correspondant aux signaux envoyés, est précisément connu le mi bémol produit.

Évidemment, l'indication qu'un son serait plus ou moins « aigu » a un sens dans le dialecte humain mais n'en a pas le moindre pour la machine – ici, le microphone qui capte le son. Les signaux que reçoit le micro n'équivalent pas à des indications humaines mais à des charges électriques. Le 0 et le 1 correspondent respectivement à un signal électrique négatif (charge de 0 Volt), et le 1 à un signal électrique positif (charge de 5 Volts). Le numérique œuvre donc par à-coups : des myriades de charges nulles et de charges faibles sont expédiées vers la machine, comme si la lumière était rythmiquement allumée puis éteinte. Au lieu de recevoir un signal continu reproduisant fidèlement l'évolution du son comme c'était le cas de la machine analogique, la machine numérique reçoit un signal discontinu.



Seulement, une fois reçue cette séquence de 0 et de 1, comment la machine est-elle en mesure de la « comprendre » si elle est dépourvue de raisonnement intellectuel ? Très simplement, cette machine doit être « numérisée » : toutes leurs fonctionnalités répondent à des séries d'à-coups électriques, soit de 0V, soit de 5V sans aucune autre option. Du seul fait de son fonctionnement, l'appareil numérique ne comprend donc que le format numérique. Ce langage numérique n'a pas à être raisonné pour être machinalement compris puisqu'il s'agit d'un langage automatique formé d'une succession de signaux électriques.

Le microphone numérique ne reproduira donc pas le son : au moment de le capter, il lui prêtera une *forme* et, ce faisant, exclura tout ce qui ne recoupe pas cette forme composée de 0 et de 1, tout ce qui n'est pas *conforme* (à commencer par le parasitisme de l'analogique). Emancipé de toute reproduction analogique, n'importe quel signal électrique peut être isolé en lui assignant un format numérique⁵⁰. Ainsi peuvent être isolées la captation de la voix (avec le microphone numérique), celle automatique du temps (avec la montre numérique), celles de la température (avec le thermomètre numérique), du son (avec le CD-ROM remplaçant le vinyle analogique), de l'image (appareil photo numérique) ... Voilà les débuts de la révolution numérique, assortie d'au moins deux conséquences tout aussi novatrices pour l'humanité.

Premièrement, **le numérique a permis l'apparition des données informatiques**. La donnée est le fruit de la transformation numérique : elle est l'unité par laquelle une suite de 0 et de 1 est arrêtée au moment où cette suite déclenche une action par la machine. Dans le cas du ténor dont on a capté la voix tout à l'heure, la suite 01101000001 représente l'action que doit réaliser le micro pour former ce que nous, humains, comprenons comme un si bémol. C'est donc cette suite qui fera sens pour la machine, et c'est celle que les êtres humains qualifieront de « donnée ». Outre le microphone, nous prendrons une autre illustration plus proche du commencement d'internet : l'ordinateur. Lorsqu'un utilisateur presse la lettre « R » de son clavier, la touche s'enfonce pour cogner contre un interrupteur situé en-deçà (même système que pour le manipulateur Morse). Une fois déclenché, l'interrupteur relié à des circuits électriques produit une succession de charges électriques – fictivement 110111011100. Dès sa conception, l'ordinateur est équipé d'un logiciel dit « système d'exploitation » qui fait coïncider le signal électrique 110111011100 avec l'enclenchement de la touche R du clavier, permettant à la machine de connaître l'action correspondante. La séquence 110111011100, en ce qu'elle provoque une action informatique déterminée, peut ainsi être considérée comme une « donnée ». Somme toute, **on définira la donnée informatique comme le résultat d'une action informatique, c'est-à-dire l'unité par laquelle peuvent être décomposées les actions exécutables par une machine numérique**. Allégoriquement, elle pourrait être symbolisée par une capsule qui contiendrait l'action informatique issue de l'envoi de signaux électriques binaires (0V ou 5V).

La donnée est l'abstraction même du numérique, elle incarne cette « forme » numérique binaire tout à fait particulière. La transformation de l'élément capté en données fait s'autonomiser l'origine du signal électrique par rapport au signal électrique effectivement retransmis : la machine numérique ignore la reproduction du monde extérieur (le son tel qu'émis), n'en connaît que la reformulation numérique (le son tel que transformé en binaire). **S'instaure une césure entre la réalité du monde extérieur et les signaux que reçoit la machine numérique. Le format numérique est créateur d'une économie interne à l'informatique, générateur d'actions informatiques propres qui ne reproduisent ni n'équivalent les actions physiques humaines**. Là où la reproduction analogique n'offrait aucune nouveauté par rapport à l'élément reproduit, le numérique forge sa propre réalité en imposant son format à l'élément capté pour l'isoler. Lorsqu'un réseau tout entier est numérisé, c'est-à-dire ses supports émetteurs/récepteurs ainsi que ses infrastructures de transport, circulent alors des données qui

⁵⁰Les techniques d'isolation ont considérablement progressé depuis, mais le principe numérique reste le même.

n'ont de sens que pour les machines numériques membres du réseau et qui traduisent des actions sans pareil en comparaison des actions physiques humaines.

Deuxième implication de la révolution numérique : son format binaire est universel. Là où les grandeurs analogiques se différenciaient d'un élément capté à l'autre (degrés pour la température, seconde/minute/heure pour le temps, décibels pour l'acoustique...), le numérique livre chaque fois le même format composé de 0 et de 1 grâce auquel peuvent être fabriqués et programmés le thermomètre, la montre, le microphone, l'ordinateur... Sur un plan pratique, tous ces objets au fonctionnement jusqu'à présent étanche gagnent la capacité de communiquer entre eux pourvu qu'ils soient tous numérisés. On entrevoit là l'annonce des objets connectés mais, bien avant, la faisabilité de transcender les différences entre machines par le numérique sera employée pour connecter une machine émettrice/réceptrice (l'ordinateur) avec les infrastructures de transport du réseau concerné (les *Interface Message Processor* pour Arpanet, les routeurs pour internet, les commutateurs de lignes téléphoniques pour le Minitel etc.). Le réseau numérique peut voir le jour.

En résumé, **la découverte du numérique a révélé la praticabilité d'un réseau électrique universel pourvu d'actions informatiques propres à sa réalité.** Chronologiquement, plusieurs réseaux numériques ont précédé internet et son extension au public : SAGE (réseau militaire), ARPANET (réseau filaire scientifico-militaire), SATNET (réseau satellite), CSNET et BITNET (réseaux inter-universitaires), USENET (réseau civil)⁵¹ ... Les héritages laissés par ces réseaux à internet ne seront toutefois pas abordés ici. Nous focaliserons le propos sur le fonctionnement d'internet, seul pertinent dans notre cadre d'étude. Le monde qui a vu le jour après la Seconde guerre mondiale est pénétré par cette révolution du réseau numérique, dont les déploiements ont été cristallisés par internet : c'est par ce réseau internet que transite la quasi-totalité des objets connectés évoqués ; le même réseau totalisait 4,54 milliards d'utilisateurs humains en 2019⁵² et il est celui des réseaux numériques qui abrite le plus de données⁵³ ; c'est aussi le réseau auquel se rattache la plupart des réseaux numériques adjacents

51 V. Intro. Pour un très bon historique des conditions politico-universitaires qui ont configuré la naissance et le fonctionnement de ces réseaux, v. FLICHY Patrice, « Internet ou la communauté scientifique idéale », *Réseaux*, n° 97, 1999, p. 79-120. Pour une histoire socio-technique de leur fonctionnement, v. notam. HAFNER Katie et LYON Matthew, *Where Wizards Stay Up Late: The Origins of The Internet*, Simon & Schuster International, 1998 et MARKOFF John, *What the Dormhouse said. How the Sixties Countercultures Shaped the Personal Computer Industry*, New York, Penguin Book, 2006. Pour une synthèse du passage d'Arpanet à internet retranscrite par l'*Internet Engineering Task Force* (IETF) – célèbre institution privée qui a pensé les fondements de l'Arpanet dans les années 1960 du temps où elle n'était qu'un groupe de chercheurs et étudiants (*Network Working Group*) et dont les standards actuellement édictés continuent d'influencer les acteurs d'internet – v. la norme *Request for Comments* (RFC) 2555, « 30 Years of RFCs », 7 avr. 1999 [en ligne sur le site de l'IETF]. Pour une histoire plus procédurale et institutionnelle du réseau internet, v. BAMDÉ Aurélien, *L'architecture normative du réseau internet. Esquisse d'une théorie*, L'Harmattan, 2014, notam. p. 59-82 puis p. 339-389

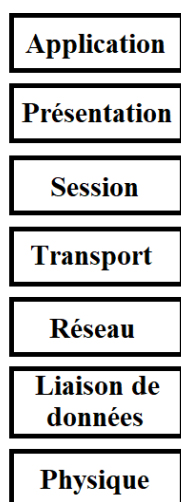
52 Hootsuite et WeAreSocial, « Digital 2020: Global Overview Report » [en ligne], *DataReportal*, janv. 2020

53 En 2020, sur une durée d'une seule minute, internet comptabilise la visualisation de 404 444 heures de vidéos Netflix, la publication de 500 heures de vidéos sur YouTube, l'envoi de 41,7 millions de messages sur WhatsApp, la création de 347 222 stories sur Instagram etc. : GAUDIAUT Tristan, « Une minute sur Internet en 2020 » [en ligne], *Statista*, 17 sept. 2020

comme des P2P⁵⁴ ou des darknets⁵⁵. Les données en réseau ont proliféré par l'universalisme et l'amplitude d'internet, étendant de la sorte une *réalité numérique en ligne* prodigieusement vaste et riche dans son étude.

C) Internet, réseau prodige

Si les phénomènes dépeints ressortent de causes numériques plus que singulièrement « internetiques », reste alors à identifier ceux qui relèvent rigoureusement du réseau internet et donc à en comprendre le fonctionnement. Ce fonctionnement sera présenté de manière à résoudre la question suivante : **comment une donnée trouve-t-elle une existence « en ligne », sur le réseau internet ?** L'étape préalable oblige bien sûr à numériser les machines, à concevoir leurs fonctionnalités conformément à des charges binaires. Les étapes suivantes sont généralement qualifiées de « couches » parce que chacune d'entre elles est pourvue d'un fonctionnement hermétique à celui des autres couches⁵⁶.



Modèle OSI (selon le standard de l'ISO) des couches, abrégées "TCP/IP"

Une fois la machine numérique mise sur pieds (étape préalable), une donnée informatique sous forme binaire pourra être produite. Cette donnée migrera d'une machine à une autre en empruntant la couche dite « physique » (**couche 1**). Le déplacement est permis par les câbles qui composent la couche 1. Ces câbles contiennent des fils conducteurs appairés⁵⁷, chacun des fils de la paire transférant, pour l'un, les signaux négatifs (0V) et, pour l'autre, les signaux positifs (5V). Le signal retransmis, encore faut-il savoir à quelle machine l'adresser : après avoir « *branché les machines* », l'étape qui suit vise à « *les faire communiquer entre elles* »⁵⁸. C'est le rôle de la couche de liaison (**couche 2**).

Deux types de matériels conditionnent le succès de cette tâche : des « matériels connectés » munis d'une adresse ; et des « matériels de connexion » qui redistribueront le signal à l'adresse pertinente. Ces matériels se rapportent aux fameuses « machines » que nous avons « branchées » en couche 1. D'une part, quant aux matériels connectés, ils sont usinés avec une adresse dite « MAC » pour *Media Access Control*. Cet identifiant unique incorporé dans chaque machine produite se lit « xx:xx:xx:xx:xx:xx », sachant que les trois premiers caractères désignent le constructeur et que l'ensemble de l'adresse s'individualise par une combinaison de chiffres allant de 0 à 9 et de lettres allant de a à f (par ex. : 00:6c:81:4f:22:ae). D'autre part, quant aux matériels de connexion, le signal électrique produit par les matériels connectés est retransmis à un commutateur, lui-même programmé avec un logiciel répertoriant dans un tableau (ou table CAM) les adresses MAC de chacun des matériels qui lui sont connectés

54 C'est le cas de l'ex-PirateBay, de CPasBien ou de T411 dont les fichiers sont accessibles depuis internet

55 C'est le cas des principaux darknets (TOR, Freenet, voire Telegram en Russie et en Inde et, par intermittence, dans d'autres pays comme l'Iran ou l'Indonésie par le passé)

56 Pour une bonne vulgarisation et mise en application de ces couches, v. LALITTE Éric, *Apprenez le fonctionnement des réseaux TCP/IP*, 4^e éd., Eyrolles, 2019

57 Originellement doubles (câbles coaxiaux), ces fils désormais au nombre de huit peuvent donc transmettre quatre signaux électriques simultanément, et sont torsadés pour protéger le signal électrique des perturbations électromagnétiques (câbles à paire torsadée)

58 LALITTE É., *Apprenez le fonctionnement des réseaux TCP/IP*, prés., 2019, p. 15-47

en couche 1 (ordinateurs, routeurs, smartphones, imprimantes, objets connectés...). Recenseur des adresses MAC, le commutateur sera le seul en mesure de jouer le rôle d'aiguilleur dans ce réseau.

Il ne pourra toutefois satisfaire sa mission que s'il a le moyen de connaître le matériel connecté émetteur et celui destinataire des données. Ce moyen lui est donné dès sa conception. Tout commutateur est programmé selon un « protocole » déterminé, *i.e.* des règles de fonctionnement à suivre. Par conséquent, les matériels connectés au commutateur ne pourront communiquer avec lui que s'ils se plient à ce protocole. Habituellement, les commutateurs suivent le protocole Ethernet qui intègre un algorithme à respecter pour les matériels connectés. En vertu de ce protocole, les données doivent parvenir au commutateur dans un certain format. Un peu comme si un administré devait remettre un dossier à l'administration pour qu'elle prenne en charge sa demande, le matériel connecté devra transmettre au commutateur Ethernet un ensemble de données. Pour un commutateur, ce « dossier » porte le nom de « trame Ethernet » et compte quatre types de données à fournir dans l'ordre suivant :

Trame Ethernet			
Adresse MAC du destinataire	Adresse MAC de l'émetteur	Données destinées à être envoyées (souvent associées au « contenu » d'un msg)	Une valeur mathématique (comme un numéro de dossier qui authentifie l'échange entre les matériels connectés émetteur et destinataire)

Avec toutes ces indications, le commutateur est en mesure de savoir où rediriger quelles données pour les faire accéder à leur point de destination de manière sécurisée et authentifiée. Toutes ces données sont évidemment converties en binaire pour que la machine numérique puisse les comprendre et accomplir les actions qui lui sont demandées. Les adresses MAC deviennent des suites de 0 et de 1 sur quarante-huit caractères dont la signification ne sera saisie que par la machine numérique. Ici s'observent pleinement les effets de la *transformation* numérique : les adresses MAC peuvent être transformées en binaire ; des « trames » peuvent être annexées au signal électrique reconverti en données... La reformulation numérique ajoute des nouveautés au signal capté, fait se distinguer les actions informatiques d'une reproduction du monde extérieur, matérialisent une réalité numérique propre. Mais le réseau Ethernet que nous venons de décrire en couche 2 n'est encore qu'un petit réseau local, un réseau domestique. C'est la couche « réseau » (**couche 3**) qui en permet l'extension publique, là où s'ouvrent les frontières d'internet.

À cet endroit, plus de protocole Ethernet mais un protocole Internet (*Internet Protocol*, IP) pour ordonner aux matériels connectés et aux matériels de connexion comment agir. Plus de commutateur pour aiguiller les données, mais des routeurs. Comment une donnée provenant de la couche 2 accède-t-elle à ce « nouveau monde » de la couche 3 ? Dès la couche 2, la trame Ethernet reçue par le commutateur fera figurer en destinataire l'adresse MAC du routeur connecté au réseau Ethernet, et inclura le protocole utilisé en couche 3 pour que la donnée soit acheminée vers le bon réseau (internet en l'espèce). Ce « routeur » connecté au réseau local correspond aujourd'hui à la célèbre *box*⁵⁹ installée dans nos habitations. Comme c'est le cas pour le commutateur Ethernet, la *box* est programmée d'après le protocole IP, contraignant ainsi

⁵⁹Qui, pour être exact, ne va pas se limiter à des activités de routage mais aussi de *modem* par la conversion en analogique de signaux numériques afin d'en permettre la transmission par voie hertzienne aux antennes-relais

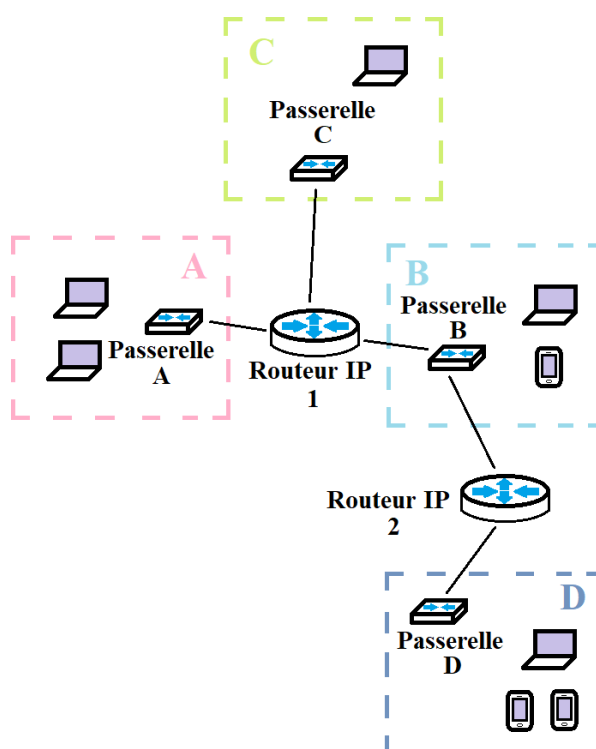
les matériels connectés à respecter les règles de ce protocole pour se faire comprendre du routeur.

Première règle de l'IP : les machines connectées au routeur doivent être adressées d'une manière spécifique à la couche 3 pour être reconnues dans cette couche. La box à la fois différenciera chacun des matériels qui lui est en connecté en lui assignant une adresse IP (par ex., 10.0.0.255), mais confèrera un point commun à chacune de ces adresses IP : un « masque de sous-réseau ». Ce masque est l'identifiant IP (par ex., 255.255.254.0) du réseau local issu de la couche 2, le « sous-réseau » par rapport au réseau de couche 3. Dans ce réseau local rattaché à une même *box*, chacune des adresses IP est donc distincte des autres mais possède le même masque de sous-réseau que les autres. Tant les matériels connectés (grâce à l'adresse IP) que le réseau local (grâce au masque IP) seront reconnaissables en couche 3 ; tout est « IP-isé » pour que puisse s'appliquer le protocole IP à l'échelle du réseau.

Les données peuvent désormais circuler au-delà du réseau local. Elles pénétreront précisément dans le réseau internet au moment d'atteindre un autre routeur. En effet, il existe deux types de routeurs : les routeurs-passerelles, avec l'exemple de la *box*; et les routeurs IP. Les passerelles comme la *box* ont pour rôle de faire l'intermédiaire avec les routeurs IP. Disposés dans les locaux des opérateurs, les routeurs IP sont paramétrés avec une table de routage, dont le principe est le même que la table CAM du commutateur Ethernet. La table de routage, toutefois, ne recensera pas des adresses MAC mais les adresses IP des réseaux auxquels le routeur est connecté. Y seront ainsi répertoriés : le masque IP du sous-réseau destinataire, pour aiguiller les données vers le réseau local pertinent ; et l'adresse IP de la passerelle appartenant à ce réseau local

destinataire, pour que les données puissent intégrer le réseau convoité.

Si le routeur IP est connecté à la passerelle destinataire, il connaît l'adresse IP ainsi que le masque du réseau destinataire et peut alors immédiatement lui transmettre les données qui passeront d'un réseau local (réseau A ci-contre) à un autre (réseau B). Si en revanche il n'est pas directement connecté à la passerelle destinataire, il fera emprunter aux données une « route par défaut » menant à celui qui, des réseaux connectés par le routeur IP, est le plus proche (réseau B) du réseau destinataire (supposons le réseau D). Le mécanisme de la « route par défaut »⁶⁰ fait ainsi ricocher les données de routeur en routeur jusqu'à ce qu'elles parviennent à destination.



⁶⁰ Les critères de la route par défaut (chemin le plus court, le plus rapide, le moins coûteux...) dépendent théoriquement du protocole auquel obéit le routeur, mais les routeurs externes comme les routeurs IP fonctionnent tous aujourd'hui avec le protocole BGP. Le protocole BGP fait choisir les routes qui traverseront le moins de réseaux, privilégie les messages venant d'un même réseau, fait emprunter un chemin stable...

Deuxième règle de l'IP: comme l'exigeait le commutateur Ethernet via la trame, les données doivent parvenir au routeur dans un format déterminé après avoir été découpées en « paquets ». Concernant cette découpe, les données projetées en ligne sont morcelées en paquets (le message « Hello World » sera par ex. découpé en trois paquets <Hel>, <lo W> et <orld>) de manière à supprimer les bruits de fond. En effet, les espaces entre les mots « Hello » et « World » étant inclus dans les paquets, ils ne représentent aucune entité numérique autonome susceptible de parasiter la transmission du signal ou d'encombrer la mémoire de la machine destinataire. Les paquets seront rassemblés à l'arrivée par le dernier routeur parcouru, qui se référera non plus à une trame Ethernet mais à un « datagramme IP » renseignant les routeurs sur diverses caractéristiques des paquets. Les routeurs IP n'auront donc qu'à lire ce datagramme reçu avec les données pour les acheminer au moyen de leur table de routage.

Datagramme (« paquet ») IP		
Adresse IP de l'émetteur	Adresse IP du destinataire	Données destinées à être envoyées

On aurait cependant tort de résumer internet à un réseau permettant l'échange entre deux réseaux locaux éloignés. Une telle réduction méconnaîtrait les couches suivantes qui, au surplus de cette faculté d'échange, fournissent celle de profiter de « services » en ligne. Hors-ligne, dans l'espace urbain, les personnes communiquent mais recourent aussi à une quantité de services (restauration, services de soins comme les pharmacies et cabinets médicaux, approvisionnement en supermarché, service de coiffure...). En ligne, la situation est la même à ceci près que les services y sont dissemblables.

Accéder à ces services suppose d'emprunter des ports fournis par la couche « transport » (**couche 4**). Au nombre de 65 535, chacun de ces ports ouvre sur des services différents – au Web, par exemple, est réservé le port 80. Leur particularité est d'appartenir à une couche entièrement logicielle, dépourvue de toute composante matérielle propre contrairement à ses prédécesseurs. Le processus matériel est antérieur. Tout comme le commutateur renvoyait les données vers la passerelle pour faire le lien avec la couche 3, le routeur fera rejoindre les données vers le port destinataire pour faire le lien avec la couche 4. Le commutateur recevait alors une trame Ethernet qui renseignait l'adresse MAC de la passerelle destinataire et le protocole de couche 3 ; de même, au moment de réceptionner le datagramme IP, le routeur obtiendra les indications du port à joindre et du protocole de couche 4. Ce protocole qui conditionnera le trajet des données en couche 4 n'est plus Ethernet ni l'IP, mais le TCP (pour vérifier en couche 4 que l'émetteur et le destinataire sont corrects) et l'UDP.

Comme précédemment, le protocole UDP crée des datagrammes (ou « segments ») UDP qui renseigneront sur le port de l'émetteur et le port du destinataire. La couche 4 étant logicielle, l'émetteur et le destinataire ne seront pas des machines mais des adresses logicielles. On opposera le terme « logiciel » à deux antonymes. Le premier, le « matériel », parce que le logiciel se superpose à la *machine* sous la forme d'un *langage* informatique avec lequel coïncident des instructions pour la machine. Le second antonyme, le « manuel », parce que le logiciel produit automatiquement des données lorsqu'il est sollicité. On définira ainsi le **logiciel** comme **un ensemble de séquences d'instructions informatiques automatiquement**

exécutables par son support⁶¹. Plusieurs illustrations de logiciels ont déjà été relatées (système d'exploitation, programme du commutateur Ethernet...), mais deux nous intéressent particulièrement en couche 4 : le logiciel créateur du service à atteindre (par ex., un site web) et le logiciel utilisé pour l'atteindre (par ex., un navigateur web). Le premier empruntera le port (80 car site *Web*) qui sera considéré « destinataire », le second empruntera le port (80 aussi car navigateur *Web*) qui sera considéré comme « source ». Les ports représentent ainsi les points de rencontre logiciels entre les membres du réseau et les services en ligne ou, plus techniquement, entre les serveurs et les routeurs. Le « serveur » n'est rien d'autre que le support d'existence d'un service en ligne, et c'est pourquoi il a sa place dans la couche suivante : la couche « application » (**couche 7**).

En effet, les couches 5 et 6 sont concrètement inexistantes dans le fonctionnement d'internet, elles relèvent d'une simple standardisation théorique issue de l'ISO (*International Standardization Organization*). Dans les faits, la couche 4 est directement reliée à la couche 7. Cette dernière abrite des serveurs, soit des machines sur lesquelles sont installés les logiciels des différents services. Comme l'ordinateur, le smartphone ou le routeur, le serveur est un matériel connecté au réseau internet et bénéficie donc à ce titre d'une adresse IP en couche 3. Or, cette situation peut susciter entre les couches 3 et 7 des incompatibilités de nature à entraver le fonctionnement du réseau internet tout entier. En effet, il est fréquent qu'un même serveur web héberge plusieurs sites web, dès lors dotés de la même adresse IP que le serveur. Comment, en couche 3, le routeur peut-il reconnaître le site web destinataire si plusieurs sites web portent la même identité ?

Ici un autre type de services que le Web vient à sa rescousse : le service « Nom de Domaines », auquel est réservé le port 53. Les serveurs dits « DNS » (*Domain Name System*) de ce service intégreront un logiciel dont la mission sera d'associer une même adresse IP numérotée à un ou plusieurs noms de domaines alphabétiques – l'adresse IP 216.58.205.3 sera par exemple associée au nom de domaine <google.fr>. En renvoyant vers le port 53, le routeur sera alors en mesure de connaître le site web destinataire, singularisé par son nom de domaine plutôt que par son adresse IP. Dans ces conditions, un **nom de domaine** peut être défini comme **une appellation donnée à un membre du réseau pour distinguer son identification de son adresse IP**. Grâce au service DNS, les couches 3 et 7 peuvent ainsi retrouver leur compatibilité, leur « interopérabilité » sans laquelle serait contrariée la praticabilité du réseau internet.

Quel que soit le service concerné (Web, Nom de domaine, Jeux-vidéos en ligne qui empruntent d'autres ports...), le serveur ne pourra être contacté au « point de rencontre » de la couche 4 que s'il est « en écoute » *i.e.* activé et opérationnel pour être ouvert sur son port d'emprunt. Le logiciel de l'émetteur (navigateur Web, programme du jeu-vidéo...) qui contactera le service à ce point de rencontre est le « client » du serveur, chaque service ayant son client attiré : le client « web » est un navigateur web (Chrome, Edge, Opera, Firefox...) ; moins utilisé aujourd'hui⁶², le client « de messagerie » (Microsoft Outlook, Mozilla Thunderbird, Mail d'Apple...) est le logiciel qui sollicitera le service Messagerie ; le client « DNS » est quant à lui programmé dans le système d'exploitation de l'émetteur etc. Par conséquent, un « service internet » qualifie simplement le logiciel « *qui est en écoute sur une machine* »⁶³ ainsi baptisée « serveur », et qu'il est dès lors possible de

61 Sans entrer dans les nuances technico-théoriques, « programme » et « logiciel » seront tenus pour synonymes

62 Moins utilisé car les boîtes mail sont désormais surtout hébergées sur des serveurs web (port 80) plutôt que sur des serveurs de messagerie (port 25). L'accès à la boîte se fait donc généralement depuis le navigateur Web.

63 LALITTE É., *Apprenez le fonctionnement...*, préc., p. 181

contacter à l'aide d'un client. Les protocoles sont profus dans cette couche 7 parce que dépendants des services concernés (protocoles HTTP ou HTTPS pour le Web qui régissent la technique de l'hyperlien, protocole SSL pour les échanges sécurisés, protocole DNS pour les noms de domaines...).

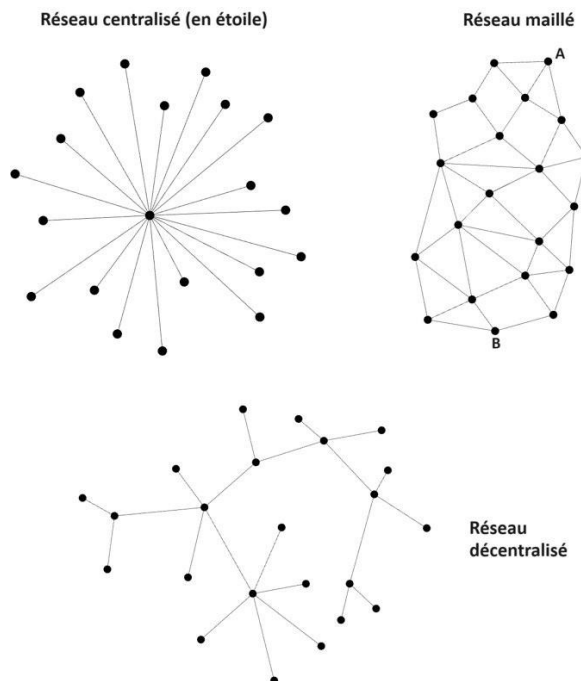
En somme, comment des données informatiques trouvent-elles une existence « en ligne » ? Prenons le cas classique de l'internaute qui souhaite produire des données sur un réseau social : puisque la donnée est le résultat d'une action informatique, il devra d'abord provoquer ladite action informatique (en cliquant sur la souris, en insérant des caractères, en tapotant sur un écran digital, en enregistrant sa voix...) depuis son client-serveur (un navigateur web s'il y accède depuis le Web, une « appli » s'il y accède depuis un logiciel installé). Le client empruntera le port pertinent (80 si navigateur web, autre si appli) et, grâce à la couche 4, rencontrera le port du service sollicité (80 si site web, 1935 pour YouTubeLive, Vimeo ou Twitch, 443 pour une grande partie des services sécurisés comme Snapchat, Twitter, Instagram etc.). Lors de cette rencontre, le client formulera une « requête » au routeur depuis la couche 3 en lui communiquant les données produites par l'internaute et en ciblant l'adresse IP du serveur à joindre. L'envoi des indications parcourt donc les couches en sens contraire : les données sont certes produites puis transférées dès la couche 1 jusqu'à la couche 7 ; mais tous les datagrammes descendront de la couche 4 à la couche 2, tous les protocoles s'appliqueront en ordre inversé de la couche 7 jusqu'à la couche 2. C'est de cette manière que la couche 4 connaît le protocole utilisé en couche 7, que le routeur de couche 3 connaît le protocole utilisé en couche 4 et les ports correspondants, que le commutateur de couche 2 connaît le protocole utilisé en couche 3. Ainsi la donnée existe-t-elle « en ligne ».

Le réseau internet objective prodigieusement la révolution du réseau numérique : les signaux électriques sont *reformulés* en datagrammes et paquets, l'identification des machines est *formalisée* par des adresses numérale, des *formats* logiciels dirigent l'activité des machines à travers les protocoles et les services... ceci dans un langage *universel* (le binaire), lui-même retraduit en langages universels par couches (les protocoles) compréhensibles par toute machine. Internet fabrique son propre *univers*, formalisé proprement. Chacune des « pièces » inspectées de ce réseau représente une part des rapports de force en ligne. Quantité de scientifiques qu'on nommera « hardwaristes » y perçoivent donc la clé de la régulation en ligne.

Paragraphe 2 - L'analyse hardwariste des rapports de force en ligne

Ce fonctionnement technique d'internet a servi d'assise commune à divers raisonnements pour la régulation d'internet, convergeant vers un même axe. Par « axe », moins qu'une école de pensée, on désignera surtout une certaine exposition de l'objet internet, un éclairage ouvert à d'autres axes. L'axe « hardwariste » soutient que, les actions informatiques en ligne pouvant toujours être ramenées à des machines en définitive, le contrôle de ces machines membres d'internet ménage un certain contrôle de ce réseau. Sous cet aspect, le premier obstacle au triomphe d'une régulation en ligne est la décentralisation du réseau internet qui dérive de son architecture maillée et décentralisée. On dénombre trois grands types d'architecture réseau : le réseau centralisé (« en étoile ») connecte une multitude de nœuds récepteurs à un même nœud émetteur ; le réseau décentralisé interconnecte les nœuds émetteurs et récepteurs à travers certains nœuds plus ou moins centraux ; le réseau distribué (« maillé ») interconnecte les nœuds émetteurs et récepteurs en répartissant les ressources informatiques entre les nœuds, de manière que les composants d'un programme et les données dépendent de plusieurs nœuds. **Internet est un réseau à la fois distribué** – les données émises depuis un point A doivent traverser les routeurs interconnectés les plus proches de la destination pour parvenir au point B, tout comme

les ressources d'un programme en ligne sont réparties entre le terminal de l'utilisateur et le serveur destinataire –, **et décentralisé** – toutes les machines membres d'un réseau local sont reliées à un nœud central (la passerelle) et on verra que des réseaux de routeurs sont parfois connectés de manière centralisée à d'autres réseaux de routeurs à travers une seule ligne de connexion (*peering*).



Une ossature maillée complique la question hardwariste en ceci qu'il n'est pas possible de contrôler chacune des machines, chacun des nœuds du réseau. Certains nœuds néanmoins déterminants ont très tôt été remarqués par les spécialistes de la régulation. Dès 1997, le juriste technophile Tim Wu, visage du hardwarisme, rappelle trois bases du fonctionnement d'internet⁶⁴. D'abord, les routeurs matérialisent les portes d'accès au réseau internet, en rendent possible la connexion et la circulation des données. De plus, les données traversent des passerelles (modems, box...) qui hébergent généralement des logiciels capables de filtrer les données dès le réseau local⁶⁵. Enfin, quel que soit le point du réseau – les infrastructures d'accès, les serveurs et fournisseurs de services en ligne, les terminaux qui se trouvent en bout de réseau et depuis lesquels sont produites les données acheminées (ordinateurs, smartphone, tablettes...) ou encore leurs périphériques (imprimantes, objets connectés...) – chacun de ces points possède un emplacement géographique. De cette triple considération, Tim Wu en conclut qu'internet n'échappe pas aux lois de la physique : si l'État contraint les activités de routage de manière à policer les connexions et accès, s'il oblige à filtrer activement les données depuis les passerelles comme le fait la Chine (l'éminent « *Great FireWall* » chinois par lequel s'opère une partie de la censure en ligne ⁶⁶), et si l'État fixe des règles géographiques de compétence du juge et

64 WU Tim, « Cyberspace Sovereignty ? ... » préc., *Harvard Journal of Law and Technology*, vol. 10, 1997, v. notam. p. 651-656

65 Les « pares-feux » ou *firewalls*, dont le rôle est en principe de sécuriser l'échange en vérifiant que les datagrammes IP/TCP/UDP sont corrects, que les services accédés sont sans danger, que les ports sont valides...

66 V. la conférence TED de ZHAO Jing (ANTI Michael, blogueur chinois militant pour les libertés numériques), « Behind the Great Firewall of China », sur *ted.com*, juin 2012

d'application de la loi, alors il pourrait juridiquement domestiquer internet. Tout cela, les États sont matériellement en mesure de le faire mais seraient arrêtés par des volontés contraires (celles de respecter les droits de l'Homme, de ne pas brimer des relations diplomatiques, par libéralisme politique ou économique...) ⁶⁷. Chercheur en sciences de l'information et de la communication, Milton Mueller insistera à son tour sur la maîtrise des machines, et particulièrement l'une d'entre elles. Il retient le serveur DNS comme le ligament principal du réseau internet en ce qu'il transporte les requêtes d'accès aux noms de domaine, et donc aux sites web. Le contrôle des routes menant aux nom de domaine assurerait dès lors un contrôle efficace des requêtes d'accès aux services, et pourrait promettre une régulation à grande échelle des atteintes aux droits de propriété intellectuelle, du commerce en ligne, des cybermenaces auxquelles internet expose les autorités nationales etc. ⁶⁸

Pour ces auteurs, la conquête étatique d'internet ne peut donc se passer des gestionnaires des infrastructures d'accès au réseau (routeurs, antennes-relais, passerelles...), *i.e.* les « opérateurs de communications électroniques ». En principe, les opérateurs sont de deux sortes : les exploitants du réseau et les fournisseurs d'accès internet (FAI). Les premiers investissent leurs activités dans la construction et l'extension de leur réseau – le plus grand réseau est détenu par Cogent Communications Inc. qui déploie de la fibre optique sur tout le continent européen et les États-Unis, et relie plus de 3 500 réseaux ou opérateurs. Les seconds, les FAI (Bouygues Telecom, SFR, Orange...), investissent leurs activités dans l'offre d'accès internet auprès de l'utilisateur final (performances de leur propre réseau, concurrence sur les prix et les services selon les attentes du consommateur...). Au réseau moins voire peu ramifié, ils doivent transiter par les réseaux des exploitants pour bénéficier d'un accès à l'internet mondial ⁶⁹. Les exploitants louent alors des services de transit aux FAI, qui empruntent ces grands réseaux moyennant rémunération.

Rapidement identifiées comme des pivots du réseau internet, les infrastructures-réseau inspirèrent des réactions juridiques très variables selon les États, mais toujours conscientes des enjeux matériels décrits. Aux États-Unis, le *Communications Assistance for Law Enforcement Act* (CALEA) de 1994 oblige les opérateurs de téléphonie et de communications électroniques à outiller leurs commutateurs téléphoniques et routeurs de logiciels scrutant les datagrammes des paquets leur parvenant (méthode dite de *deep packet inspection*) pour en permettre l'accès en temps réel aux services d'enquêtes criminelles ⁷⁰. Plutôt que l'accès en temps réel, la France privilégie un accès différé après conservation, c'est-à-dire contraint les opérateurs à sauvegarder un « stock » de données dans lequel pourront puiser les services d'enquête judiciaire pour la recherche et la poursuite d'infractions. Obligatoire depuis 2001 ⁷¹, ce stock contient des données techniques identifiantes qui environnent le contenu des messages, plus simplement « métadonnées » : les données de connexion (date et heure de production des données, géolocalisation

67 GOLDSMITH Jack L. et WU Tim, *Who Controls the Internet: Illusions of a Borderless World*, Oxford University Press, 2006

68 MUELLER Milton L., *Ruling the Root. Internet Governance and the Taming of Cyberspace*, MIT Press, 2002

69 Certains FAI se sont considérablement étendus depuis, nous y reviendrons

70 DALY Angela, « The Legality of Deep Packet Inspection », *International Journal of Communications Law and Policy*, vol. 14, 2011

71 Loi n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne, art. 29 créateur de l'art. L32-3-1 de l'ancien Code des postes et télécommunications, devenu l'art. L34-1 du Code des postes et des communications électroniques (CPCE) depuis sa refonte par la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle

des terminaux émetteur et destinataire, durée d'un appel, mode de connexion wifi...) et les données de trafic (adresses MAC et IP de l'émetteur et du destinataire, numéros de téléphone des appelés et appelants, services accédés...),⁷² Si l'opérateur entend garder une trace de ses clients pour sa comptabilité ou pour de potentiels litiges – c'est constamment le cas dans les faits –, il enrichira ce stock des données de facturation (adresses postale et mail de l'abonné, coordonnées bancaires, référence du contrat...) conservables aussi longtemps que dure la relation contractuelle avec l'abonné dans la mesure où elles sont pertinentes⁷³. En 2004, la loi pour la confiance dans l'économie numérique (LCEN) fait peser ce devoir de conservation sur un chaînon supplémentaire du réseau : les serveurs, et particulièrement les personnes dites « hébergeurs » qui les mettent à disposition des internautes (Instagram, Twitter, TikTok...) ou des entreprises (location de leurs serveurs par OVH, Hostinger, LWS...)⁷⁴.

Par la même loi, les serveurs et infrastructures-réseau deviennent également les colonnes d'appui de la régulation des contenus. À la charge⁷⁵ des hébergeurs et opérateurs, l'art. 6, I, 8 de cette loi confie au juge le pouvoir de prononcer « *toute mesure* » destinée à faire cesser ou prévenir un dommage provoqué par un contenu. La LCEN de 2004 généralise en cela l'initiative prise en référé par le Tribunal de Grande Instance de Paris en 2000 par laquelle le juge ordonnait à la société Yahoo! de « *prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation [par les utilisateurs français] sur Yahoo.com (...) d'objets nazis et de tout (...) site ou service qui constitue une apologie du nazisme ou une contestation des crimes nazis* »⁷⁶. Dans la jurisprudence française, l'art. 6, I, 8 LCEN suggérera au juge trois types de mesures. Le *blocage* s'ordonne à l'opérateur (les routeurs empêchent l'acheminement des données vers le service hébergeant le contenu litigieux ou vers l'URL qui renvoie au contenu) ; la *suppression* s'ordonne à l'hébergeur (les données litigieuses sont supprimées des serveurs détenus par l'hébergeur) ; et le *déréférencement* s'ordonne au moteur de recherche (les données sont retirées de la liste des résultats depuis les serveurs du moteur de recherche)⁷⁷. Les machines membres du réseau ont ainsi été appréhendées comme un enjeu de pouvoir en ligne par la grande majorité des ordres juridiques qui en ont les moyens : en Russie, depuis 2019, la méthode de *deep packet inspection* est

72 Art. R10-13 et R10-14 CPCE

73 Art. L34-1, IV CPCE

74 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, art. 6, II. Les hébergeurs *français* (TGI Paris, ord., *UEJF c. Twitter*, 24 janv. 2013) sont alors tenus de conserver les identifiants de connexion (adresses IP), la nature de l'opération (création, modification, suppression de données...), l'identifiant de l'objet de l'opération (URL, référence d'un article publié ou d'une réaction en ligne...), l'identifiant utilisé par l'auteur de l'opération le cas échéant (adresse mail, pseudonyme de connexion au service...), les dates et heures de l'opération et les protocoles utilisés pour la connexion au service : décret n° 2011-219 du 25 fév. 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, art. 1^{er}

75 Y compris financière depuis CA Paris, Pôle 5, *Allotstreaming e. a.*, 15 mars 2016, n°14/01359 confirmé par C. Cass., *Allotstreaming e. a.*, 6 juil. 2017, arrêt n° 909

76 TGI Paris, ord., *UEJF, LICRA et MRAP c/ Yahoo! Inc. et Yahoo France*, 20 nov. 2000

77 TGI Paris, ord., *PMU c/ Computer Aided Technologies*, 2 nov. 2005 (pour l'une des premières applications de blocage sur le fondement de la LCEN) ; CA Montpellier, 5^e ch. sect. A, *Jean-Marc D. c/ JFG Networks*, 15 déc. 2011 (pour un exemple de suppression ordonnée à l'hébergeur) ; TGI Paris, ord., *APC e. a. c/ Auchan Telecom e. a.*, 8 nov. 2013 (pour la première application du déréférencement sur le fondement de la LCEN)

employée pour bloquer l'accès à des sites web inscrits sur une « liste noire »⁷⁸ ; en Chine continentale, les infrastructures-réseau n'ont pas pu se déployer sans que l'État y fasse installer des logiciels de filtrage⁷⁹.

Toutefois, penser la *régulation* par les machines, c'est aussi penser les *droits et libertés en ligne* par les machines comme le revendiquent plusieurs auteurs. En 2003, T. Wu théorise le concept de « neutralité du Réseau » par lequel il invite les États et opérateurs à ne pas conditionner l'acheminement des données selon l'émetteur ou le destinataire⁸⁰. Pour les opérateurs, ce principe leur interdit d'utiliser les capacités de transmission de leurs infrastructures pour privilégier certains services en ligne au détriment d'autres services. Pour les internautes, le principe de neutralité leur reconnaît, dans la mesure des capacités de transmission de l'opérateur, l'égal pouvoir de profiter de n'importe quel terminal, de n'importe quel service, depuis ou vers n'importe quel lieu géographique. Ce principe qui cantonne les infrastructures-réseau à un rôle passif d'acheminement ne cesse d'évoluer théoriquement, recevant des déclinaisons de la part de certaines autorités de régulation. Pour nous en tenir à la France, depuis 2018, l'Autorité de régulation des communications électroniques et des postes (Arcep) qui régule l'activité des opérateurs français milite activement pour une « *neutralité des terminaux* »⁸¹. Le rapport de l'Arcep questionne : l'utilisation des terminaux est-elle vraiment libre si les systèmes d'exploitation verrouillent certains paramètres ; si des programmes préinstallés par les fabricants ne peuvent être désinstallés ; si le terminal n'a plus le choix du réseau de transport, alors que des sociétés comme Amazon réservent l'accessibilité de certains de leurs services aux terminaux empruntant leur réseau exclusif (phénomène de *kindle-isation*) ? La neutralité du Réseau et ses déclinaisons représentent ainsi une sorte de « liberté-cadre » qui, à la source (matérielle) du réseau, établit une utilisation d'internet libérée des intérêts privés.

Positivement reçu par le droit européen, quoique restreint aux seuls FAI à l'exclusion des autres opérateurs, le principe de neutralité du Réseau est consacré le 25 novembre 2015 par le règlement 2015/2120 (UE) dit « pour l'accès à un Internet ouvert ». D'un côté, sont inscrites la liberté des utilisateurs de recourir aux terminaux ou d'accéder aux services de leur choix indépendamment du lieu géographique des uns et des autres, et l'interdiction pour les FAI de brimer cette liberté via leur contrat avec l'abonné (en augmentant ou diminuant les prix d'accès à un service ou le débit binaire accordé à un service etc.). La première interprétation jurisprudentielle de ce règlement en a donc logiquement tiré l'inconventionnalité des offres dites *zero rating* (« trafic gratuit » ou « dé-tarification »)⁸², fréquentes sur le marché de l'accès internet, par lesquelles un FAI ne facture pas à l'abonné l'accès à certains services (vidéos YouTube illimitées, écoutes gratuites sur Spotify...) aux dépens des autres services. De l'autre côté, hors de tout enjeu contractuel, l'art. 3.3 du règlement interdit aux FAI de discriminer l'acheminement des données selon l'identité de l'émetteur ou du destinataire, les contenus consultés, les services accédés ou les terminaux

78 Loi fédérale n° 90 FZ modifiant la loi fédérale relative aux communications et la loi fédérale relative à l'information, aux technologies de l'information et à la protection de l'information du 1^{er} mai 2019, Art. 1^{er}, 3) c)

79 ZITTRAIN Jonathan L., EDELMAN Benjamin G., « Empirical Analysis of Internet Filtering in China », sur *cyber.harvard.edu*, 2003

80 WU Tim, « Network Neutrality, Broadband Discrimination », *Journal on Telecom and High Tech Law*, vol. 2, 2003, p. 141-175

81 Arcep, Rapport « Smartphones, tablettes, assistants vocaux... Les terminaux, maillon faible de l'ouverture d'internet », fév. 2018, p. 5 [en ligne]

82 CJUE, *Telenor Magyarország*, 15 sept. 2020, aff. C-807/18

utilisés. La mise en œuvre de ce règlement par la France a complété les missions de l'Arcep, chargée depuis la loi pour une République numérique (LRN) de 2016⁸³ de vérifier le respect par les opérateurs de la neutralité du réseau internet ainsi définie et des règles concurrentielles qui en découlent.

Autre droit-cadre réclamé par une partie de l'axe hardwariste : la *Privacy by Design*. Après sa collaboration avec l'Organisation néerlandaise pour la recherche scientifique appliquée et l'Autorité néerlandaise de protection des données en 1995⁸⁴, Ann Cavoukian donne naissance à l'expression une fois devenue commissaire à l'information et à la protection de la vie privée de l'Ontario en 1997. Le rôle préventif de la *Privacy by Design* vise à faire respecter les règles de vie privée des utilisateurs dès la conception de la machine ou du logiciel, l'obligation pesant alors sur le fabricant, l'équipementier et/ou le responsable du développement du logiciel. Une fois de plus, ce concept a connu des dérivations, notamment après avoir été accusé de déresponsabiliser l'internaute sur sa propre vie privée et d'engendrer des coûts excessifs pour les services et les industriels au grand dam d'une égale concurrence. Pour ces raisons, les économistes Alain Rallet et Fabrice Rochelandet et la juriste Célia Zolynski lui préfèrent une *Privacy by Using* qui obligerait les acteurs concernés, non plus à préprogrammer des règles de vie privée par défaut, mais à fournir aux internautes des technologies leur permettant de connaître l'utilisation faite de leurs données personnelles⁸⁵.

Le droit positif ne semble pas pour l'heure très sensible à la *Privacy by Using*, mais la *Privacy by Design* est quant à elle protégée par le droit de l'Union Européenne depuis 2016 à travers l'article 25 du Règlement Général pour la Protection des Données personnelles (RGPD). Plus précisément, ce règlement concerne les personnes physiques ou morales qui appliquent un « traitement », i.e. une opération informatique quelle qu'elle soit (collecte, conservation, suppression, modification, extraction, transfert, utilisation...), à des données identifiantes pour leur producteur. Dans ce cas, l'article 25 fait obligation à ces « responsables de traitement » de fournir des machines et services : qui, *par défaut*, rendent ces données inaccessibles aux tiers (sous-traitants, partenaires, co-contractants revendeurs de données...), ne proposent de collecter que celles nécessaires aux finalités de l'opération et suppriment celles ne l'étant plus ; et qui, *en eux-mêmes*, ne collectent que les données nécessaires aux finalités de l'opération, sécurisent ces données identifiantes (en les pseudonymisant, en veillant à corriger les vulnérabilités des matériels et logiciels...) et limite leur accès à des personnes déterminées (par ex., par une procédure d'habilitation)⁸⁶.

Mises à part l'approche strictement régulatoire ou celle libérale, une troisième approche hardwariste étudie les machines par le biais des couches TCP/IP. À leur examen, T. Wu note que ces couches certes remettent aux infrastructures d'accès le pouvoir sur l'existence en ligne

83 Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique, art. 40

84 HES Ronald, BORKING John J., « Privacy-Enhancing Technologies: The Path to Anonymity », *Information and Privacy Commissioner of Ontario*, 1995

85 RALLET Alain, ROCHELANDET Fabrice, ZOLYNSKI Célia, « De la Privacy by Design à la Privacy by Using : regards croisés droit/économie », *Réseaux*, n° 189, 2015/1, p. 15-46

86 DESGENS-PASANAU Guillaume, *La protection des données personnelles. Le RGPD et la nouvelle loi française*, LexisNexis, 2018 (3^e éd.), p. 43 : « Concrètement, ce principe implique que les données traitées soient limitées à ce qui est strictement nécessaire au regard de la finalité du traitement, que des durées de conservation aient été fixées, qu'il existe des règles de suppression automatique des données et qu'un processus d'habilitation soit mis en place pour l'accès aux données personnelles au bénéfice des seules personnes ayant à en connaître »

des données, mais attribuent le « *pouvoir de codage* »⁸⁷ en ligne aux concepteurs d'applications de la couche 7. Les acteurs d'internet sont alors observés à l'échelle de leur couche d'appartenance. À cette échelle, Lawrence B. Solum et Minn Chung estiment qu'une régulation pertinente d'internet serait celle faisant respecter la séparation des couches en sorte qu'aucun acteur ne puisse s'accaparer plusieurs couches, ni ne puisse perturber leurs principes de fonctionnement respectifs ou leur harmonisation, leur interopérabilité. L'interopérabilité des couches a également suscité l'intérêt d'économistes comme Thierry Pénard qui y voit la cause d'une interdépendance économique entre acteurs d'une même couche et entre acteurs de couches différentes⁸⁸. Pour un exemple, l'opérateur Open Transit relie son réseau à celui de l'exploitant Cogent et à celui du FAI Orange, faisant ainsi le pont entre l'exploitant et le FAI. La société Cogent subira donc les répercussions des capacités de trafic proposées par Orange. Mécontent d'une mauvaise qualité de trafic, l'exploitant n'a ainsi pas hésité à saisir le juge pour se plaindre d'un « *mécontentement des internautes* » et d'un « *détourn[ement] des clients de Cogent* »⁸⁹. La qualité du trafic tient alors de la combinaison d'interdépendances techniques, de relations contractuelles et de considérations économiques par lesquelles les opérateurs se contrôlent mutuellement. En raison de l'architecture en couches, les acteurs d'internet en seraient des régulateurs *de fait* car techniquement contraints par l'interopérabilité, ce qui imposerait à la régulation étatique d'être plus partageuse. Par conséquent, cette approche « protocolaire » par couches conduit souvent les scientifiques qui l'adoptent à des conclusions proches de l'autorégulation, de l'inter-régulation (coordination des diverses autorités de régulation) ou de la co-régulation (association des acteurs publics et privés pour la discussion, la décision et l'action réglementaires⁹⁰). Tenant compte de ces implications de l'architecture en couches, le législateur européen a fixé des exigences communes d'interopérabilité aux opérateurs dès 1997⁹¹.

En substance, l'axe hardwariste conçoit donc les acteurs d'internet, non comme étant « internes » au réseau, quittant leur condition physique externe, mais au contraire comme des acteurs redevables de machines d'où la régulation peut voire doit être mise à exécution. La machine distancie le réseau de ses acteurs : pour Dan Hunter, le vocable « cyberspace » n'est qu'une vue de l'esprit qui, par analogie linguistique, assimile un objet (le réseau internet) à un lieu qui n'en est pas un ; internet désigne un réseau numérique qui fonctionne au moyen de machines et de câbles⁹². L'acteur d'internet serait avant tout un *utilisateur de machines*. Un second axe, qui se distingue de celui hardwariste, s'accorde sur cette même conclusion, recherchant toutefois les causes d'une régulation efficace moins auprès de la « machine » qu'auprès de l'« utilisateur », particulièrement de l'utilisateur humain. Cette différence au départ de l'analyse

⁸⁷ WU Tim, « Application-Centered Internet Analysis », *Virginia Law Review*, vol. 85, 1999, p. 1193

⁸⁸ PÉNARD Thierry, « Faut-il repenser la politique de la concurrence sur des marchés internet ? », *Revue internationale de droit économique*, 2006/1, p. 57-88

⁸⁹ CA Paris, Pôle 05 ch. 7, 19 déc. 2013, n° 2012/19484

⁹⁰ V. par ex. la thèse de Luca Belli pour qui l'architecture en couches rend incontournable une régulation « multi- » et « hétéro-parties prenantes » : BELLI Lucas, *De la gouvernance à la régulation de l'internet*, Berger-Levrault, 2016, v. notam. p. 144s.

⁹¹ Directive 97/33/CE du 30 juin 1997 relative à l'interconnexion dans le secteur des télécommunications en vue d'assurer un service universel et l'interopérabilité par l'application des principes de fourniture d'un réseau ouvert. Par application, en France, c'est l'Arcep née la même année qui est gardienne des exigences d'interopérabilité (art. L. 32-1 CPCE).

⁹² HUNTER Dan, « Cyberspace as Place and the Tragedy of the Digital Anticommons », *California Law Review*, vol. 91, 2003, p. 439-519

emporte une différence analytique à l'arrivée : le trait physique qui sépare le réseau internet de ses acteurs n'est plus la machine, mais le caractère humain des seconds.

Section 2. La distanciation du réseau et de ses acteurs par leur humanité selon l'axe social

D'autres rapports de force régissant le réseau internet ont été retenus comme le résultat d'activités économiques et sociales (Paragraphe 1) ou d'informations en ligne qui acquièrent une signification sociale (Paragraphe 2).

Paragraphe 1 - La lecture pragmatique des rapports de force en ligne

La lecture pragmatique, qui localise les sources du pouvoir dans les pratiques des acteurs d'internet, place le curseur de la régulation sur leurs activités, commerciales (A) ou institutionnelles (B).

A) Enjeux pratiques des fournisseurs de services en ligne

Le pragmatisme auquel nous faisons référence résonne avec celui porté par le juge américain et icône du mouvement *Law and Economics* Richard Posner, appartenant à l'École libérale de Chicago. Suivant sa lecture pragmatique, R. Posner pose d'abord le regard sur l'office des notions (*proposals*) qui lui sont soumises, leur rôle fondamental, leur raison d'être. Aussi l'office du Droit ne se résumerait pas à exécuter des règles ; ces règles de droit auraient fondamentalement pour rôle de servir l'humanité, du moins dans une démocratie. En droit, « *ce qui fonctionne* » (*what works*) serait alors conjugué à ce qui est profitable à la prospérité et au bonheur d'une personne⁹³. Or, aucune réponse systématisée, telle que celle énoncée par une loi, ne peut être apportée à ce questionnement configuré par les circonstances. En tant qu'elles sont systématiques, les théories quelle qu'elles soient (juridiques, philosophiques, économiques, politiques...) ne permettraient pas de résoudre les problèmes qui naissent des circonstances.

Dans une vie humaine, les journées seraient immobiles si des théories en dictaient le déroulement. Si ce n'est que les journées ne sont pas immobiles *en pratique* : elles sont guidées par des faits, des incidences, des accidents, des pensées, des comportements qui en singularisent l'écoulement. Par cette projection, R. Posner invite le juge à embrasser un « *pragmatisme quotidien* » (*everyday pragmatism*) : un litige est aussi singulier que peut l'être une journée, et aucune théorie, aucun systématisme ne devrait en déterminer l'issue. Le juge devrait, à l'aune des circonstances de l'espèce, arrêter sa décision selon « *ce qui fonctionne* » en droit, tel que sus-défini. Cela ne signifie pas que le juge est libre de prendre n'importe quelle décision. Pour des « *raisons instrumentales* »⁹⁴, le respect du précédent est une nécessité juridique, une part intégrante du Droit. Partant, le juge n'interrogera pas pragmatiquement la règle du précédent comme il devra interroger pragmatiquement le litige.

L'appréciation du juge pragmatique est alors pilotée par des facteurs extra-juridiques qui incombent à **la réalité pratique, à ces circonstances qui défient l'immobilité théorique**. R. Posner l'illustre par la jurisprudence avec le cas du juge de *common law* qui, saisi d'un dysfonctionnement du marché, « *mime* » les résultats efficients auxquels le marché aurait pu

93 POSNER Richard, *Pragmatism, Law and Democracy*, Harvard University Press, 2003, p. 50

94 SULLIVAN Michael et SOLOVE Daniel J., « Can Pragmatism Be Radical ? Richard Posner and Legal Pragmatism », *The Yale Law Journal*, vol. 113, 2003, p. 694

mener si son fonctionnement n'avait pas été contrarié⁹⁵. Plus généralement, le juge anglo-saxon serait imprégné par les lois du marché lesquelles, de la sorte, s'immiscent comme « pratiques » dans le jeu juridique. Il ne serait rien d'absolument autonome sans que la pratique en infléchisse la direction : les éléments de notre monde auxquels le Droit ne fait pas exception s'interpénétreraient, tout serait « désordonné »⁹⁶, toute catégorisation serait relative.

Internet ne fait pas exception non plus : peut-être est-il producteur de sa propre réalité (sociale, numérique, systémique...), mais il est aussi le fait de pratiques extérieures et, en cela, est hétéronome comme toute chose. De là, les pragmatiques en déduisent qu'internet n'est pas imperméable au Droit, qu'il est juridiquement régulable à partir de ses pratiques. Dan Farber approfondira en ce sens l'application du pragmatisme posnerien au réseau internet. D'après lui, les données sont comparables à des marchandises ; si on réussit à juguler le marché international des biens, on peut réussir à juguler le marché international des données⁹⁷. Dans ce sens, endiguer internet présupposerait de réguler les nouveaux « compétiteurs » de ce « marché des idées ». La régulation opérerait alors moins auprès des machines, comme le préconise l'axe hardwariste, qu'auprès des comportements des acteurs d'internet. Que ces comportements soient rapportés à des jeux concurrentiels (comme l'entrevoit Dan Farber) ou non, ils partagent la même racine humaine rappelée par Michel Vivant : « si l'on parle de cyberspace ou de monde virtuel, il n'en demeure pas moins que cet espace est un espace humain, comme tel appelant « régulation », encadrement si l'on préfère, relevant donc du droit (sauf à juger que seule doive régner la loi du plus fort) »⁹⁸. La plausibilité de la régulation en ligne tient de la nature *in fine* humaine de ses acteurs et de leurs pratiques d'internet.

Une analyse pragmatique d'internet pré-requiert donc de cibler ces fameux « acteurs d'internet », leur rôle et leurs agissements en société (humaine). En société, c'est par les contrats que les opérateurs étendent leurs réseaux. En effet, il ne suffit pas à l'exploitant de disposer d'infrastructures d'acheminement éparpillées dans le monde pour agrandir son réseau ; encore lui faut-il relier ces infrastructures pour qu'elles puissent s'échanger les flux de données que chacune reçoit, *i.e.* leur trafic respectif. Les conditions et l'existence même de cet échange sont stipulées par des contrats dits de *peering*. En reprenant l'illustration de l'exploitant Cogent, parmi les milliers d'opérateurs qu'il connecte, un⁹⁹ se situe à New York, un autre à Paris ; ces deux derniers opérateurs signeront un contrat de *peering* avec Cogent par lequel ils s'engagent à partager leur trafic ; de cette façon, les données reçues par l'opérateur new-yorkais pourront être retransmises directement à l'opérateur parisien, sans détour par un autre opérateur. Plus un réseau entend s'agrandir, plus l'opérateur qui le gère doit recourir au *peering* pour

95 KIRAT Thierry, « Le pragmatisme de Richard Posner : un regard critique », texte provisoire de la communication la journée d'étude *Les philosophes pragmatistes et les économistes : quelles proximités ?*, IDHE-ENS de Cachan, 11 avr. 2005 [en ligne sur HAL]

96 BUTLER Brian Edgar, Entrée « Legal Pragmatism », *Internet Encyclopedia of Philosophy* [en ligne sur l'IEP]

97 FARBER Daniel C., « Expressive commerce in cyberspace : public goods, network effects, and free speech », *Georgia State University Law Review*, 2000, p. 791 : « Internet est à la production de la culture locale ce que le commerce international est à la fabrication locale de biens. En permettant l'importation et l'exportation d'informations, Internet élargit le " marché des idées ", introduisant ainsi de nouveaux concurrents et permettant une production plus efficace, mais aussi mettant en péril les valeurs des communautés locales » (trad. libre)

98 VIVANT Michel, Fiche « Internet », *Répertoire de droit international*, Dalloz, 2017, §1

99 Plusieurs en réalité, nous singulariserons les opérateurs pour simplifier l'exemple

interconnecter son réseau à d'autres. Cette pratique des contrats de *peering* a bouleversé l'état du marché à long terme : grâce aux recettes de leurs activités, les FAI ont pu étendre leurs réseaux à l'aide du *peering*, devenant capable depuis la fin des années 2000 de louer leur transit auprès de réseaux plus petits et se transformant pour certains en concurrents directs des exploitants.

La régulation du marché des opérateurs s'est adaptée en conséquence. Ainsi en France l'Arcep ne contrôle-t-elle plus les opérateurs selon qu'ils seraient des FAI ou des exploitants, mais selon leurs relations contractuelles. L'Arcep ajuste désormais son intervention régulatrice selon trois catégories d'opérateurs¹⁰⁰. D'abord, les opérateurs de rang 1 (ou les « Tier 1 » ou *transit free*), qui sont au nombre de 9 à 20, englobent les détenteurs d'un réseau longue distance suffisamment interconnecté au niveau mondial et concluant des accords de *peering* à échelle internationale. Ensuite, les opérateurs de rang 2 (ou les « Tier 2 ») visent les gestionnaires de réseaux qui, de taille moyenne, sont contraints de payer des services de transit aux Tier 1 et de restreindre leurs accords de *peering* à leur zone géographique. Enfin, les opérateurs de rang 3 (ou « Tier 3 » ou *transit only*) désignent des opérateurs dont le réseau est de petite taille et dont la connectivité dépend exclusivement du recours au transit des Tier 1, en sorte qu'ils ne concluent pas d'accord de *peering* avec d'autres opérateurs. L'autorité publique de régulation appréhende de cette façon les opérateurs d'après leurs pratiques contractuelles, qu'elles aient pour objet le transit (emprunt d'un réseau tiers) ou le trafic (transmission des flux de données).

Ce glissement d'une régulation collée à la technique (dichotomie exploitants/FAI) vers une régulation alignée sur les usages sociaux des acteurs (contrats de *peering* et de transit) vaut plus profondément encore pour le régime de responsabilité de ces acteurs à l'égard des contenus. Le régime ici en cause ne couvre plus les données telles qu'acheminées par les opérateurs sous forme de signaux électriques numérisés (les « communications électroniques »), mais les données arrivées à destination telles qu'elles apparaissent à la compréhension humaine (le « contenu en ligne » qui renvoie non plus aux communications électroniques mais aux « communications au public en ligne » ou CAPEL).

La responsabilité de l'acteur est échelonnée selon sa capacité technique à connaître le contenu. Le FAI est exonéré de toute responsabilité d'un contenu illicite tant qu'il se borne à transmettre les données (activité de transport) ou à mettre à disposition des serveurs-relais sur lesquels sont stockés les services les plus demandés pour accélérer leur accès lorsque leur hébergement est géographiquement éloigné (activité de cache). L'hébergeur est en principe irresponsable aussi longtemps qu'il se limite à héberger le service et les contenus, mais retrouve sa responsabilité engagée lorsqu'il n'a pas retiré rapidement de ses serveurs certains contenus illicites dont il a eu effectivement connaissance. Les autres fournisseurs de services en ligne voient leur responsabilité automatiquement retenue pour un contenu illicite dès lors que leur activité est propice à la connaissance dudit contenu (sites web de presse qui modèrent préalablement les commentaires publiés, blog qui publie les articles d'utilisateurs après les avoir vérifiés...). Ce triple régime de responsabilité issu des sections 223 et 230 du *Communications Decency Act* américain de 1996

100Pour une illustration, v. Arcep, avis n° 2011-1241 du 20 oct. 2011 répondant à la demande d'avis de l'Autorité de la concurrence portant sur la saisine de la société Cogent en date du 9 mai 2011 relative à des pratiques mises en œuvre par la société France Télécom sur le marché du transit et ses marchés connexes

est aussi motivé par des considérations économiques¹⁰¹, outre celles initialement techniques. Ainsi déresponsabilisés, les FAI et hébergeurs peuvent se développer sans que leur essor économique soit freiné par les contenus venus des internautes. Par harmonisation avec les États-Unis, la directive européenne 2000/31 du 8 juin 2000 sur le commerce électronique reprend cette « irresponsabilité conditionnelle » avec deux nuances : les « autres fournisseurs de services » deviennent des « éditeurs », ce qui ne change pas grand-chose dans les faits¹⁰² ; plus substantiellement, l'Union Européenne étend la responsabilité de l'hébergeur à tout contenu illicite effectivement connu, là où la loi américaine n'envisageait que trois exceptions à l'irresponsabilité de principe¹⁰³.

Au moment de transposer ces dispositions de la directive 2000/31 par la LCEN, le législateur français centre à son tour le débat sur des enjeux technico-économiques après avoir auditionné opérateurs, hébergeurs et industriels du secteur. Soulignant l'architecture maillée distinctive du réseau internet¹⁰⁴, il voit dans les opérateurs et hébergeurs des « intermédiaires »¹⁰⁵ et module la responsabilité des acteurs selon leur capacité technique à connaître le contenu¹⁰⁶. Ce régime inspiré de la technique évoluera progressivement au gré des pratiques sociales, notamment celles des hébergeurs. D'une part, l'emploi massif des moteurs de recherche et leur rôle déterminant dans l'accès aux contenus ont poussé le juge français à dissocier ces acteurs des autres hébergeurs pour leur appliquer des mesures spéciales de déréférencement [v. *supra*]. D'autre part, pour réagir face à l'émergence de « Grand-Places numériques » détenues par des oligopoles (Amazon, Google, Facebook, AirBnB, eBay, Snapchat, Uber, Twitter...) dont l'émergence inquiétait déjà la doctrine dans la première moitié des années

101Il suffit de lire les (A) et (B) de la section 230(c) pour s'en convaincre : « *c'est la politique des Etats-Unis : (1) de promouvoir le développement continu de l'Internet, et des autres services informatiques interactifs [interactive computer services, notion qui regroupe les FAI et hébergeurs] et des autres médias interactifs ; (2) de préserver le marché libre, dynamique et concurrentiel qui existe actuellement pour l'Internet et les autres services informatiques interactifs, sans être entravés par une réglementation fédérale ou étatique* »

102Théoriquement, contrairement aux Etats-Unis, un opérateur ne peut relever de cette catégorie qui enclenche automatiquement la responsabilité du contenu ; le droit européen en arrive pour autant au même résultat, puisque l'irresponsabilité de l'opérateur ne vaut que pour ses activités de transport ou de cache ; hors de ces activités, l'opérateur est susceptible d'agir de manière à connaître le contenu auquel cas sa responsabilité sera impliquée

103Cette irresponsabilité tombe si le contenu (i) viole la loi criminelle fédérale ou (ii) contrevient aux lois relatives à la propriété intellectuelle si l'hébergeur n'a pas retiré promptement le contenu contrefacteur qui lui est signalé, ou (iii) si l'hébergeur viole l'*Electronic Communications Privacy Act* en permettant l'accès non-autorisé à une communication électronique stockée par un service de communications électroniques.

104Sénat, Commission des affaires économiques, *Rapport législatif n° 345*, 11 juin 2003, p. 32 : « *la communication audiovisuelle est une communication point/multipoint, tandis que la communication publique en ligne est une communication point-à-point, fournie sur demande individuelle* »

105Assemblée Nationale, Commission des affaires économiques, de l'environnement et du territoire, *Rapport législatif n° 612 (1^e partie)*, 12 fév. 2003, p. 23 : « *le Code pénal (...) permettrait de sanctionner les intermédiaires hébergeant ou transmettant un contenu lorsqu'ils se faisaient complices de la diffusion d'un contenu dont ils connaîtraient le caractère illicite* »

106Sénat, Commission des affaires économiques, *Rapport législatif n° 232*, 3 mars 2004, p. 25 : « *le régime de responsabilité de l'hébergeur est beaucoup plus large que celui du fournisseur d'accès, dont la responsabilité est assimilée à celle d'un transporteur par l'article 12 de la directive* »

2010¹⁰⁷, l'art. 49 de la loi pour une République numérique (LRN) de 2016 sépare des autres hébergeurs les « plateformes », aux obligations d'information alourdies auprès des consommateurs-utilisateurs. Tant pour les opérateurs que pour les hébergeurs, la régulation initialement adossée à la technique tend à se fixer sur les pratiques sociales de ces acteurs.

B) Enjeux pratiques des acteurs institutionnels publics et privés d'internet

Cette régulation pragmatique repose alors prioritairement sur l'identification des acteurs « incontournables » d'internet par le prisme de leurs pratiques. Maints chercheurs sont donc partis à la « source » du réseau pour en extraire les deux « ressources critiques d'internet », c'est-à-dire les ressources nécessaires à l'échange minimal de données sur ce réseau. Premièrement, les adresses IP permettent aux machines membres du réseau de se reconnaître réciproquement afin de se communiquer les données en circulation. Deuxièmement, les noms de domaine leur sont indispensables pour distinguer les services présents en ligne voire les terminaux au sein d'un groupe d'utilisateurs lorsque ce groupe est coiffé d'une même adresse IP. Chacune de ces deux ressources critiques est administrée par un même gestionnaire : un organisme international de droit privé répondant de l'acronyme « Icann » (*Internet Corporation for Assigned Names and Numbers*), historiquement placé sous la tutelle du Département du Commerce américain à sa création en 1999 jusqu'à son autonomisation en 2009. Quant aux adresses IP, l'Icann en vérifie la régularité, inventorie celles attribuables et délègue contractuellement aux FAI la livraison des adresses IP auprès des réseaux locaux. Quant aux noms de domaine (par ex. <google.com>), ils sont scindés au niveau de leur suffixe (<.com>) et de leur préfixe (<google>).

L'Icann garde la main sur la création de nouveaux « suffixes », à la qualification plus appropriée de « *Top Level Domain* » (TLD). Les enjeux de cette activité de l'Icann sont à la fois géopolitiques, économiques et sociaux. Géopolitiques d'abord, parce que la création d'un TLD peut rivaliser avec les souverainetés étatiques et les équilibres territoriaux. Par exemple, la naissance d'un <.bzh> réservé à la Bretagne ou d'un <.paris>, tous deux distincts du <.fr>, attente-t-elle à l'indivisibilité du territoire français préservée par l'art. 1^{er} de la Constitution du 4 octobre 1958 ? De même, les autorités étatiques peuvent-elles être placées sous un régime de nommage identique à celui d'autorités politiques non reconnues comme des États par le droit international, telle la Palestine ? C'est l'Icann qui a répondu à ces questions, en admettant la réservation d'un TLD par des localités (ccTLD comme <.bzh>¹⁰⁸, <.paris>...) mais en refusant une telle réservation par la Palestine, n'accordant un <.ps> qu'aux territoires palestiniens occupés au titre des ccTLD¹⁰⁹ et non au titre des geoTLD spécifiques aux pays (<.fr>, <.uk>...). La création d'un TLD s'accompagne ensuite d'enjeux économiques : un TLD se référant à une activité déterminée (tel que le <.wine>) peut-il être disponible à l'usage de personnes étrangères à cette activité (telles que des personnes extérieures au marché du vin) ? Malgré les protestations du gouvernement français dénonçant la concurrence déloyale qu'engendrerait le <.wine> pour les producteurs de vin français, l'Icann a validé la création et la disponibilité de ce TLD au titre

107Par ex., KIM Nancy S. et TELMAN Jeremy, « Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent », *Missouri Law Review*, vol. 80, 2015, p. 723-770

108Création du <.bzh> le 27.02.2014 : <https://www.icann.org/resources/pages/registries-date-2013-09-18-en>

109Création du <.ps> tranchée par l'Icann le 22.03.2000 : <https://www.iana.org/domains/root/db/ps.html>

des gTLD (TLD génériques universellement exploitables comme <.com>, <.net>, <.org>...) ¹¹⁰. Sont enfin concernés des enjeux sociaux dès lors que la création d'un TLD est évaluée par des objecteurs internes à l'Icann à l'aune d'un « *limited public interest* » indéfini, sorte d'ordre public. Mais en désaccord avec l'ordre public français qui y verrait sans doute une violation de la dignité humaine, pourrait tout à fait être jugé conforme à ce *limited public interest* un TLD de type <.mortauxflics> ou <.acab> (*all cops are bastards*) dès lors que les objecteurs sont libérés dans leur appréciation de toute contrainte juridique comme en témoigne l'ex-objecteur Alain Pellet ¹¹¹. Spécialiste français du droit des noms de domaines, Cédric Manara synthétisera pour nous : dans toutes les situations décrites, « *l'État est entièrement suspendu aux décisions d'une entité étrangère de droit privé [l'Icann], qui a présidé à sa création et à son attribution, et pourrait théoriquement décider de sa destruction* » ¹¹².

Si l'Icann reste maître de la création des TLD, elle délègue généralement leur gestion à des *registries* : la gestion du <.com> est cédée au *registry* VeriSign ; celle des <.paris> et <.fr>, à l'Association française pour le nommage internet en coopération (Afnic), une association loi-de 1901 de droit privé mandatée par le gouvernement français. Concrètement, tout enregistrement ou renouvellement de noms de domaines en <.fr> ou <.paris> doit obtenir l'autorisation de l'Afnic qui en vérifiera la conformité par rapport à l'ordre public ¹¹³. Aux côtés des *registries*, des *registrars* se voient à leur tour délégué par l'Icann l'enregistrement non plus des TLD mais des *Second Level Domain*, ou SLD, qui incluent cette fois le préfixe devant le TLD (<google.com> est un SLD dont <.com> est le TLD). Dans les faits, un candidat à l'obtention d'un SLD adresse directement sa demande à un *registrar* (Gandi, Indom, GoDaddy...) qui, par contrat avec des *registries* (VeriSign, Afnic...), est autorisé à commercialiser les TLD tenus par ces *registries* cocontractants. Aux *registries*, l'Icann leur fait signer des *Registry Agreements* par lesquels elle assure sa prééminence sur les délégataires, par exemple avec une clause-type qui soumet à l'approbation de l'Icann « *toute révision d'un accord passé entre un registry et un registrar* » ¹¹⁴. Aux *registrars*, elle leur fait signer des *Registrar Accreditation Agreements* dont une clause-type leur interdit par exemple d'enregistrer un nom de domaine contraire à la politique de l'Icann et à son interprétation du *limited public interest* ¹¹⁵. L'Icann impose ainsi contractuellement sa prééminence sur les étages inférieurs, voire sa « *politique* » en remontant des *registries* jusqu'aux *registrars* ¹¹⁶.

Techniquement identifiée à partir des ressources critiques, la position incontournable de l'Icann est pragmatiquement déduite de ses activités – contractuelles ou de production et

110 Sur l'opposition entre l'Icann et le gouvernement français, v. la lettre du directeur de l'Icann adressée à la secrétaire d'Etat chargée du Numérique, Axelle Lemaire, en date du 22.10.2014 : <https://www.icann.org/en/system/files/correspondence/chehade-to-lemaire-22oct14-fr.pdf>. Sur la mise en circulation du <.wine> à partir du 18.06.2015 : <https://www.icann.org/resources/agreement/wine-2015-06-18-en>

111 PELLET Alain, « Une gestion privée de l'ordre public de l'internet ? », in PELLET A. (dir.), *Internet et le droit international*, Colloque de Rouen, Editions A. Pedone, 2013, p. 239-249

112 MANARA Cédric, « Nom des personnes publiques et droit de l'Internet », *Communication Commerce Electronique*, n° 3, 2016, p. 11

113 Art. L45-2, 2° CPCE

114 V. par ex. art. 2.9 du contrat autorisant certains registry à gérer le gTLD <.wine> : <https://www.icann.org/sites/default/files/tlds/wine/wine-agmt-pdf-18jun15-en.pdf>

115 V. section 3.7.6 du I : <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

116 BAMDÉ A., *L'architecture normative du réseau internet*, préc., 2014, p. 376

validation de TLD. Ce glissement qui a précédemment été observé pour les hébergeurs et opérateurs est très net chez les tenants du pragmatisme. Bertrand du Marais convient en ce sens que, si le DNS représente « *l'infrastructure essentielle du réseau* » (poids technique), il est aussi « *possible de démontrer que le nommage [est] bien un service public* » (activité)¹¹⁷.

Que l'analyse pragmatique porte son regard sur les opérateurs, hébergeurs ou l'Icann, elle repère la puissance d'un acteur d'internet selon son activité mise en pratique¹¹⁸. Dans ce schéma de pensée, une régulation pragmatique entraîne naturellement une régulation sectorisée selon les activités concernées. Emblème de cette régulation pragmatique d'internet, la LCEN la tronçonne par secteurs d'activité (couverture-réseau du territoire¹¹⁹, activités commerciales en ligne¹²⁰, responsabilité selon les activités d'hébergement ou d'accès internet...). Les conclusions auxquelles en arrive le courant pragmatique côtoient alors celles retenues par l'approche « protocolaire » de l'axe hardwariste, à savoir la pertinence d'une co-régulation. Dans son rapport « *Internet et les réseaux numériques* » de 1998, le Conseil d'État avise ainsi le législateur : « *dans le cas de l'Internet, qui ne relève pas d'une traditionnelle logique de diffusion, il semble préférable de s'orienter vers la combinaison d'un co-régulation avec les professionnels, sous le contrôle du juge, pour encadrer les services propres au réseau (...), et de la régulation habituelle des services traditionnels concernés* »¹²¹. Dupliquant cet extrait dans ses débats, le législateur de la LCEN en appelle à une « *régulation des services de l'Internet préservant les régulations sectorielles* »¹²².

Internationalement, le pragmatisme s'est épanoui dans une logique *multistakeholder* : à l'issue du 2^e volet du Sommet Mondiale pour la Société de l'Information de 2005 qui a réuni les 193 États, l'art. 34 de l'Agenda de Tunis définit consensuellement la « *gouvernance de l'internet* » comme « *l'élaboration et l'application par les États, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de internet* ». Cette « *gouvernance* » d'internet appelant l'intervention d'acteurs privés comprend certes l'Icann, les hébergeurs et opérateurs, mais aussi les organismes de normalisation du réseau.

Auprès des développeurs de logiciels, le W3C (*World Wide Web Consortium*) – fondé en 1994 par Tim Berners-Lee, l'inventeur du service Web (protocole HTTP diffusé en 1991), avec le soutien fédéral des États-Unis et celui de la Commission européenne – propose des langages informatiques standards (HTML5, XML, PNG...) conçus pour être interopérables avec le protocole du Web. Rédigés à partir des formules issues de ces standards, les logiciels s'exprimeront ainsi

117DU MARAIS Bertrand, « Le service public du nommage, consécration et limites », *Revue française d'administration publique*, n° 146, 2013, p. 299

118Par ex., en ingénierie informatique : MOUNIER Pierre, *Les Maîtres du réseau*, La Découverte, 2002. En gestion informatique : FAYON David, *Géopolitique d'Internet*, Economica, 2013. Pour ces auteurs, les activités de l'Icann et les pratiques des sociétés commerciales dominant le marché de la technologie en réseau assoieraient la puissance de ces acteurs dans les rapports de force en ligne.

119L'art. 52 LCEN reconnaît à cette fin un nouveau pouvoir de police administrative aux collectivités locales : celui d'ordonner à un opérateur de fournir une couverture réseau 2G dans les zones identifiées comme « non couvertes » par le préfet de région en concertation avec les départements et opérateurs

120LCEN, Titre II (art. 14 à 28)

121Conseil d'Etat, Rapport « Internet et les réseaux numériques », 2 juil. 1998, p. 164-165

122Assemblée Nationale, Rapport législatif n° 612 préc. [*supra* note], p. 15

dans un langage compréhensible selon les règles du protocole HTTP, et pourront alors fonctionner correctement sur le Web. Auprès des opérateurs et constructeurs, l'IETF (*Internet Engineering Task Force*) – né en 1969 du très informel *Network Working Group* réunissant les créateurs de l'Arpanet – propose des standards RFC (*Request for Comments*) relatifs à l'architecture du réseau internet (évolutions des protocoles, interopérabilité des infrastructures-réseau, améliorations du système d'adressage IP...). Préparées par l'IETF selon une procédure délibérative interne¹²³, ces RFC s'aident des recherches menées par un organe de l'IETF, l'IRTF (*Internet Research Task Force*), et sont ensuite validées par un autre de ses organes, l'IESG (*Internet Engineering Steering Group*). Le travail de ces trois ensembles est synchronisé par l'IAB (*Internet Architecture Board*), lui-même placée depuis 1992 sous la tutelle de l'*Internet Society*. Issue des inventeurs du TCP/IP Vinton Cerf et Bob Kahn, l'*Internet Society* est une organisation non lucrative qui rencontre les gouvernements pour répandre et faire appliquer les standards techniques des RFC en accompagnant les États dans la formation aux technologies en réseau et l'égal accès à internet dans le monde. Du fait de la réception favorable d'un certain nombre de RFC sur le marché de la construction et des infrastructures-réseau, et d'une large adoption des langages web selon les normes du W3C, plusieurs chercheurs citent ce complexe normalisateur dont les standards sont les plus profus comme déterminant dans les rapports de force en ligne¹²⁴.

L'application du pragmatisme à internet s'est plus récemment modernisée avec le succès du concept d'interrégulation promu par Marie-Anne Frison Roche¹²⁵. Par croisement des diverses régulations sectorielles, ce projet espère faire confluer toutes celles afférentes au réseau internet en coordonnant les autorités administratives indépendantes intéressées¹²⁶. Par exemple, une publicité personnalisée en ligne peut aussi bien relever de la Commission nationale de l'informatique et des libertés (CNIL) si elle repose sur du traitement de données personnelles, que de l'Autorité de la concurrence si la publicité a été réalisée dans des conditions faussant le libre jeu concurrentiel ; à supposer que cette publicité se fasse au profit de jeux d'argent et de hasard en ligne (Unibet, Betclac...), l'Autorité Nationale des Jeux sera elle aussi compétente ; l'annonce pourrait même ressortir du champ de compétence du Conseil supérieur de l'audiovisuel si elle était déposée sur un média audiovisuel à la demande (Netflix, services de *replay*...). Suite logique du pragmatisme, l'interrégulation relie les autorités nées de la

123L'IETF est composé de sept Secteurs (*Areas*) dans lesquels sont répartis une cent-trentaine de groupes de travail. Une RFC provient d'une charte (*Birds of a Feather Meeting*) proposée par l'un au moins des groupes de travail, laquelle charte doit ensuite recevoir homologation du Directeur de Secteur compétent (*Area Director*), pour enfin être soumise aux autres groupes de travail pour amendement et vote. Durant la période d'amendement, la charte est mise en ligne sous la forme d'un *Internet Draft* conviant toute personne à participer à la discussion de cette RFC en projet. À l'issue du vote, l'*Internet Draft* devient officiellement une RFC.

124Par ex., en sciences de l'information et de la communication : MASSIT-FOLLÉA Françoise, « Standards Agreements and Normative Collisions in Internet Governance » in MASSIT-FOLLÉA F., MÉADEL Cécile et MONNOYER-SMITH Laurence (dir.), *Normative Expérience in Internet Politics*, Presse des Mines, 2012, p. 69-92 (qui dénonce des conflits d'intérêts parmi les participants à l'IETF). En ingénierie des réseaux électriques : BACCELLI François, « Le réseau de communication du futur », *Annales des Mines – Réalités industrielles*, 2010/4, p. 9 : « les contours de l'Internet du futur seront la résultante de plusieurs vecteurs de gouvernance : la standardisation, la normalisation, les forums et les blogs, les décisions des acteurs économiques et les décisions des gouvernements ».

125FRISON-ROCHE Marie-Anne, « L'hypothèse de l'interrégulation » in FRISON-ROCHE Marie-Anne (dir.), *Les risques de régulation*, Vol. 3, Dalloz, 2005, p. 69-80

126FRISON-ROCHE Marie-Anne (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016

sectorisation pragmatique, édifiant par-là un « réseau régulateur » capable d'appréhender le plus transversalement des acteurs d'internet eux-mêmes entrelacés par leurs activités. Les « acteurs d'internet » sont alors remarqués dans leurs *activités*, leurs pratiques en société (humaine). Au-delà de ces pratiques mais tout aussi collée à la société humaine, une autre lecture porte davantage le regard sur les données comme cellules de régulation.

Paragraphe 2 - La lecture informationnelle des rapports de force en ligne

La lecture informationnelle pose la réflexion régulatrice sur les données elles-mêmes, observées en qualité d'informations humainement préhensibles, soit matériellement (A) soit immatériellement (B).

A) La donnée-information saisie matériellement par l'être humain

Une régulation informationnelle encadre les données, non à l'état numérique telles que binairement comprises par les machines, mais en société humaine telles qu'elles informent la personne humaine. « Informer » sera ici pris dans son sens le plus étymologique de « donner forme » (du verbe latin *informare*). Dans cette lignée, selon le dictionnaire en ligne du Centre national de ressources textuelles et lexicales, le verbe « informer » vise l' « action de donner ou de recevoir une forme ». Une forme rend ainsi saisissable une « réalité concrète ou abstraite »¹²⁷, rend possible d'unifier cette réalité – la *donner*, en créant un mot, en dessinant un pourtour... – ou d'y accéder – la *recevoir*, en lisant un mot, en regardant un dessin... Suivant ces repères lexicaux, **on nommera « information » toute forme saisissable par son donneur ou son récepteur**. Il en découle que les déclinaisons « informer », « être informé » et « s'informer » signifieront respectivement pour nous « fournir une forme saisissable par son donneur ou son récepteur », « recevoir une telle forme » et « accéder par soi-même à une telle forme déjà fournie ». Puisque la lecture informationnelle qui nous occupe étudie l'information en société humaine, on ramènera ici l'information à toute forme saisissable par un donneur humain ou un récepteur humain.

Un premier embranchement « économique » de cette lecture observe que l'information portée par une donnée informatique met à disposition de la personne humaine une forme matériellement saisissable selon les caractéristiques d'un « bien » (ou d'un service). En cette qualité, l'information humainement extraite d'une donnée peut être manipulée comme l'est un bien, par exemple en faisant l'objet d'une appropriation, d'une valorisation, d'un échange...

Pour le premier penseur de la cybernétique, Norbert Wiener [1948], l'information ne doit faire l'objet d'aucune appropriation, ni étatique par la voie militaire, ni privée par la marchandisation¹²⁸. Sur ce dernier point, les instabilités du marché seraient constitutives d'entropie (de *désordre*) sociale ; or, l'information consiste à mettre de l'ordre par la forme, à corriger l'entropie générée par le bruit, « manifestation naturelle de l'entropie dans le message »¹²⁹ ; rendre l'information tributaire des instabilités du marché, de l'alternance de ses acteurs économiques aliènerait ladite information à l'entropie, l'empêcherait de remplir sa mission de mise en ordre. Autre source d'entropie que le marché, en écho à la Seconde Guerre

¹²⁷CNRTL, Entrée « Forme » dans l'onglet « Lexicographie » [en ligne]

¹²⁸LE ROUX Ronan, « L'homéostasie sociale selon Norbert Wiener », *Revue d'histoire des sciences humaines*, n° 16, 2007, v. p. 121-124

¹²⁹ *Ibid.*, p. 123

Mondiale : l'aléa politique dont rien ne pourrait empêcher qu'il emporte le monde entier dans ses décisions irrationnelles car engageant « *des significations humaines (malheur, trahison...) et des conséquences sociales* »¹³⁰. Ne désignant qu'une mise en forme rationnelle car automatique, l'information serait humainement neutre *per se*. Plus l'échange d'informations serait libéré et autorégulé (hors-marché), moins l'entropie et le risque de chaos auraient de prise sur la société. Par sa théorie et ses propositions, « *Wiener renoue avec une vieille thématique libérale, celle de la paix par l'échange, qu'il adapte cependant au contexte informationnel en excluant toute forme d'appropriation de l'information* »¹³¹. À travers l'échange et le risque d'appropriation des informations, N. Wiener prête à ces dernières les attributs d'un bien.

Prendre l'information pour un bien peut aussi faire naître des aspirations contraires à celles de N. Wiener, en insufflant par exemple la volonté de s'approprier des informations. Retraçant le parcours de cette volonté propriétaire, Benjamin Loveluck constate l'essor d'un « *renouveau libéral* » depuis les années 1970 qui¹³²

« *témoigne d'une volonté de faire circuler l'information, fondée non seulement sur l'idée que la communication est le meilleur garant de la liberté individuelle, mais qu'elle est également source de développement économique. (...) À la société de l'information correspondrait ainsi une "économie de la connaissance" ou "économie du savoir" qui ferait suite au "capitalisme industriel". (...) L'innovation et la création notamment, en tant que transformation de la nouveauté en valeur économique, acquièrent un rôle décisif, ainsi que la protection de celles-ci à travers les droits de propriété intellectuelle. Cette problématique (...) touche à un des piliers du libéralisme : la propriété privée. C'est donc également une articulation clé dans la définition du libéralisme informationnel tel qu'il se manifeste sur internet* ».

Favorisé par le droit positif, ce positionnement de l'information au cœur des rapports économiques résulte d'un tournant historique décidé à la fin du XVIII^e siècle. Au siècle précédent, en 1662, l'Angleterre adoptait le *Licensing Act* qui interdisait toute impression – c'est-à-dire toute reproduction et publication – non consignée dans le Registre des Papèteries. Du même coup, les papèteries étaient pleinement habilitées à faire jouer leur droit de propriété sur les moyens d'impression pour exclure un auteur ou ses écrits du Registre. L'intensification de la censure et les protestations des auteurs ont amené le législateur anglais de 1710 à voter le *Statute of Anne* qui, du droit de propriété plein et entier des éditeurs, en a fait un droit de propriété limité, partagé avec les auteurs¹³³. D'une part, pour les 14 années qui suivaient la publication d'un écrit (28 si l'auteur restait en vie passé ce premier délai), son auteur se voyait reconnaître un « *droit de propriété* ». Concrètement, pour la première fois depuis l'apparition de l'État moderne, l'auteur bénéficiait d'un droit exclusif quant à la reproduction de son œuvre,

¹³⁰*Ibid.*

¹³¹LOVELUCK Benjamin, *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Armand Colin, 2015, p. 25

¹³² *Ibid.*, p. 91-92

¹³³JOYCE Craig P. et PATTERSON L. Ray, « Copyright in 1791: An essay Concerning the Founders' View of the Copyright Power Granted to Congress in Article I, Section 8, Clause 8 of the US Constitution », *Emory Law Journal*, vol. 52, 2003, p. 915

droit qu'il avait la liberté de céder. D'autre part, ce délai épuisé, l'éditeur récupérait les droits de reproduction de l'écrit de manière à en assurer l'impression après la mort de l'auteur.

Une première étape est franchie par le *Statute of Anne*¹³⁴ : le droit de propriété provient d'une source non plus matérielle (les *outils* d'impression de l'éditeur) mais immatérielle (la *décision* de l'auteur de reproduire son œuvre). L'étape suivante sera franchie par la France. Inspiré en 1789 par le rapporteur de Boufflers dans le contexte de la future première loi sur les brevets d'invention et pour qui « *s'il existe pour un Homme une véritable propriété, c'est sa pensée* », le Roi Louis XVI sanctionnera le décret des 31 décembre 1790-7 janvier 1791 relatif aux auteurs de découvertes utiles énonçant : « *Toute idée nouvelle dont la manifestation ou le développement peut devenir utile à la société appartient primitivement à celui qui l'a conçue / [art. 1^{er} :] Toute découverte ou nouvelle invention est la propriété de son auteur* »¹³⁵. La « *pensée* », l'« *idée* » devient objet du droit de propriété là où l'Angleterre et les États-Unis avaient soigneusement limité toute aliénation du savoir par une propriété privée exclusive.

Alors que « *les NTIC transform[e]nt le savoir en information et permett[e]nt sa circulation à l'échelle mondiale* »¹³⁶, la donnée informatique ou plutôt l'information qui lui est annexée peut ainsi devenir objet de propriété. Pour qu'une telle évolution soit opérante en droit, est évidemment pré-requise la qualification juridique de la donnée informatique en « *information* ». En France, ce sera chose faite dès 1981 par un arrêté ministériel définissant l'informatique comme la « *science du traitement rationnel, notamment par machine informatique, de l'information considérée comme le support des connaissances et des communications dans les domaines technique, économique et social* »¹³⁷. Dix ans plus tard, l'Union Européenne reconnaît le droit des auteurs à fixer sur leurs œuvres des « *mesures techniques de protection* » ou *Digital Rights Management* (DRM), *i.e.* des dispositifs techniques incorporés à l'œuvre protégée pour en empêcher ou en limiter certains actes d'utilisation (tels des dispositifs intégrés à la cassette VHS empêchant l'enregistrement tout numérique en direct depuis une émission TVHD, ou d'autres dispositifs obligeant la saisine d'un mot de passe pour accéder à l'œuvre, interdisant sa modification, rendant l'œuvre illisible à l'utilisateur qui n'a pas payé pour son accès etc.)¹³⁸. Cette directive 91/250 reste néanmoins prudente sur toute hypothèse d'appropriation privée des données. Elle qualifiait certes la donnée d'« *information* » pour définir l'interopérabilité matériel/logiciel (cons. 11, art. 6) mais ne reconnaissait pas proprement un droit de l'auteur sur une « *information* », et ne concevait pas la mise en circulation comme une liberté mais comme une atteinte potentielle aux droits d'auteur (art. 7). Une décennie supplémentaire devra s'achever pour que la **directive 2001/29** rende le droit de propriété de l'auteur exerçable sur des données en qualité

¹³⁴Repris mot pour mot par le premier *Copyright Act* américain de 1790, lui-même inspiré de la *Copyright Clause* inscrite dans la Constitution des États-Unis de 1787 faisant du Congrès le régulateur des droits d'auteur (art. I, Sect. 8 Cl. 8) et s'expliquant en partie par la crainte d'un retour à la censure éditoriale des papèteries sous le règne abrégé du *Licensing Act*

¹³⁵BLAIZOT-HAZARD Catherine, « *Savoir et droits fondamentaux – De l'ère industrielle à l'ère communicationnelle* », *RFDA*, n° 4, 2016, p. 708s.

¹³⁶*Ibid.* p. 714 (l'auteure note au passage que l'information est une « *notion plus large que le savoir* », p. 715)

¹³⁷Arrêté du ministre de l'industrie et du ministre de l'éducation nationale sur l'enrichissement du vocabulaire de l'informatique du 22 décembre 1981, *JORF* du 17 janv. 1982, p. 625

¹³⁸Directive 91/250 du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur, dont les dispositions relatives aux DRM sont sensiblement reprises par les Traités sur le droit d'auteur et sur les interprétations et exécutions et les phonogrammes de l'Organisation Mondiale de la Propriété Intellectuelle de 1996 et par le *Digital Millenium Copyright Act* américain du 28 oct. 1998

d' « informations » issues de réseaux numériques, d'une « société de l'information » régie par la « liberté de circulation »¹³⁹. **La donnée est juridiquement métamorphosée en information appropriable au titre du droit d'auteur.** Illustration topique relevée par Fabrice Mattatia : par crainte de se voir intenter un procès sur le terrain de la propriété intellectuelle, Larousse dût renoncer à publier son ouvrage *Les perles des tweets et du net* recensant des tweets marquants, utilisés sans l'accord de leurs auteurs¹⁴⁰. La même direction a été prise en 2007 par le Conseil de l'Europe à l'occasion d'un arrêt de la Cour européenne des droits de l'Homme (Cour EDH) qui allègue la « valeur économique » d'un nom de domaine pour le qualifier de « bien » appartenant à son propriétaire en vertu de l'art. 1^{er} du Premier protocole de la Convention européenne des droits de l'Homme (Conv. EDH)¹⁴¹.

Aussi, en devenant « information » la donnée devient-elle un « bien ». Déjà en 1984, Pierre Catala avisait : « *L'information est un bien créé et non pas donné, c'est un produit de l'activité humaine (...) mais les éléments régulièrement captés ne deviennent information véritable qu'à travers le deuxième terme de l'appropriation : la formalisation qui les rend communicables* »¹⁴². On notera que l' « information » en tant que bien n'est pas tenue pour antonyme de l' « activité humaine » primée par l'analyse pragmatique. Une fois encore, ces éclairages ne sont pas incompatibles. Leur combinaison la plus récurrente, ici exprimée par P. Catala, fait résulter l'information d'une activité humaine. M.-A. Frison Roche actualisera cette position mi-informationnelle mi-pragmatique. S'appuyant sur la définition de la donnée personnelle comme « *information identifiante* » posée par le RGPD et son ancêtre la directive 95/46, elle reproche à ces textes d'avoir fait de la donnée personnelle une marchandise en qualité d' « *information* » placée sous le régime communautaire de la liberté de circulation. L'Union Européenne fonde en ceci le droit d'exploiter une donnée personnelle sur les propriétés informationnelles affectées à la donnée¹⁴³. Conformément au pragmatisme, la régulation d'internet impliquerait alors celle de cette activité, de la pratique de ce droit d'exploiter économiquement de telles données : « *indépendamment de son origine ou de son format, chaque donnée renferme une information qui est la matière première de toute activité d'exploitation de données* »¹⁴⁴. Le régime des données personnelles, autant que celui des droits d'auteur en ligne, transforment ainsi la donnée-numérique en une donnée-information saisissable matériellement par l'Homme à la manière d'un bien économiquement valorisable.

139Sur la « société de l'information » : mentionnée dans le titre de la directive 2001/29 sur l'harmonisation du droit d'auteur et des droits voisins dans la société de l'information, aux cons. 2 à 20, et déterminant le champ d'application à l'art. 1^{er}. Sur la « liberté de circulation » : v. cons. 6 et cons. 57 croisé avec l'art. 5.2. o)

140MATTATIA Fabrice, *Droit d'auteur & propriété intellectuelle dans le numérique*, Eyrolles, 2017, p. 24

141Cour EDH, *Paeffgen GmbH c. Allemagne*, 19 sept. 2007, n° 25379/04

142CATALA Pierre, « Ebauche d'une théorie juridique de l'information », *Recueil Dalloz*, 1984, p.99 [on souligne]

143FRISON-ROCHE Marie-Anne (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016, p. 12 : « le Droit communautaire conçoit ainsi [la donnée] : une valeur économique disponible dans une société de consommation d'information »

144PUIGVENTOS Rémi, « L'exploitation du big data comme enjeu de souveraineté numérique », in TÜRK Pauline et VALLAR Christian (dir.), *La souveraineté numérique. Le concept, les enjeux*, Mare & Martin, 2017, p. 110

B) La donnée-information saisie immatériellement par l'être humain

Un second embranchement « communicationnel » de la lecture informationnelle fait correspondre la donnée binaire à une information appropriable immatériellement, saisissable par l'entendement humain. La puissance d'un acteur d'internet n'est plus mesurée par l'appropriation matérielle de l'information, mais par l'impact de cette dernière sur la compréhension humaine. N'est pas seulement concernée la compréhension immédiate, instantanée d'une information (la blessure morale ressentie après réception d'un contenu haineux par ex.) mais aussi sa compréhension à long terme, socialement implantée. Sur le long terme, exprimée, une information contribuerait au façonnement d'une société humaine. Étymologiquement, une information est *exprimée* si elle jaillit sous l'effet de la pression – du préfixe latin *ex-* (sortie) et du verbe *premo* (presser). Une personne s'exprime si elle accentue un point (sur une peinture, sur son accoutrement, dans ses récits...) pour le faire ressortir ¹⁴⁵. Autrement dit, l'« **expression humaine** » désigne la capacité de l'être humain à s'extérioriser par quelque moyen que ce soit (l'action, le vêtement, la parole...).

Les incidences sociales de cette faculté expressive sont illustrées par la sociologue Zeynep Tufekçi. Premier exemple : dans une société exclusivement orale ou ignorant l'écriture, les jeunes ne peuvent pas acquérir de nouveaux apprentissages par la lecture et tiennent donc leurs connaissances des personnes âgées qui ont cumulé et assimilé davantage de connaissances ; une telle société prendrait spontanément une orientation gérontocratique comme c'est généralement observé pour les sociétés peu alphabétisées. Deuxième exemple : dans une société technologisée, l'expression humaine est transportée par des technologies (diligences, chemins de fer, bateaux, voitures...) qui « *modifient aussi notre sens de l'espace (...). Les révoltes qui secouèrent l'Europe en 1848 (...) ne furent pas seulement liées à l'émergence des journaux et télégraphes, mais aussi aux chemins de fer qui ont émaillé de plus en plus le continent, transportant non seulement des gens qui transportent des idées, mais aussi des journaux, pamphlets et manifestes.* »¹⁴⁶. La société humaine et ses mutations procèdent, au moins pour partie, de l'expression de ses membres. Jürgen Habermas attribue même l'origine de toute société humaine à la communication¹⁴⁷. Depuis le postulat kantien fondant la société humaine sur la Raison de ses membres, J. Habermas en déduit que, si les êtres humains ne s'exprimaient pas, les Raisons humaines ne pourraient communiquer ni donc faire société. Toute communication constituerait en cela une *action* dans la construction sociale. Par sa théorie de l'« *agir communicationnel* », le philosophe brise l'opposition classique entre l'acte et la parole : s'exprimer, c'est agir socialement ; inversement, toute société s'actionne par la communication. L'école habermassienne pense la communication comme l'action par laquelle l'être humain extériorise sa Raison pour la partager avec d'autres et former ainsi une société¹⁴⁸.

145Dictionnaire Gaffiot français-latin, Entrées « Expressus »/« Exprimo », 1934, p. 633 [en ligne sur [lexilogos](#)]

146TUFEKCI Zeynep, *Twitter and Tear Gas : The Power and Fragility of Networked Protest*, YUP, 2017, p. 40

147HABERMAS Jürgen, *Théorie de l'agir communicationnel* (1981), Fayard, trad. fr. 1987 (t. I) et 1997 (t. II)

148De là en est tirée une théorie contractualiste fondée sur l'idée d'une conscience collective (nationale pour l'Etat-Nation) formée par l'action et la raison communicationnelles de ses membres, et de laquelle communication découlerait le « *contrat social* » par lequel des Hommes se reconnaissent

Pour vérifier la pertinence de ces diverses explications vis-à-vis d'internet, restait à expérimenter la réalité de comportements sociaux inclinés par les nouvelles technologies de *l'information et de la communication* en tant qu'elles transportent des expressions humaines. Les réseaux sociaux ont été parmi les principaux objets d'expérimentation sociologique à cette fin. Avant même l'essor d'internet, François Héran examine plusieurs réseaux de sociabilité (collègues de travail, cadre familial...) et, confirmant les résultats d'études française et californienne, constate que plus un tel réseau est fermé, moins nombreux y seront les échanges mais plus fortes y seront les relations interpersonnelles ; inversement plus un tel réseau est ouvert, plus nombreux seront les échanges mais plus faibles seront les relations interpersonnelles. La « *densité des échanges au sein d'un milieu* », i.e. au sein d'une communauté, d'un réseau de sociabilité, et la « *densité des réseaux interpersonnels* » suivent des courbes contraires¹⁴⁹. Des combinaisons et variations peuvent s'en déduire : si un réseau de sociabilité est ouvert, il a plutôt intérêt à multiplier les liens faibles¹⁵⁰ (connaissances, rencontres, commentaires-réactions...) s'il veut densifier les échanges qu'il accueille ; inversement, s'il est fermé, c'est par l'affermissement des liens forts (amis, famille...) que sera maximisée la densité des échanges. En 2016, les conclusions d'une enquête menée cette fois sur le réseau social Facebook corroborent la justesse de ce schéma dans le cadre d'internet : en priorisant les publications de proches dans le fil d'actualité, l'algorithme *Edge Rank* de Facebook optimise le nombre d'échanges par la consolidation de liens forts existants, quasiment sans création de liens forts nouveaux et avec une stabilisation des liens faibles¹⁵¹.

Les technologies de la communication en réseau ne circonscrivent pas leurs incidences sociales à une fluctuation des liens forts ou faibles. Les *usages* mêmes des objets technologiques seraient téléguidés par l'information en ligne. Depuis le renouvellement de la sociologie des usages dans la deuxième moitié des années 1990, l'« usage » ne désigne plus tant une utilisation passive de l'objet technologique que son « *appropriation* » par l'utilisateur¹⁵², c'est-à-dire les « *significations* » que transporte l'objet « *dans le contexte des pratiques de vie quotidienne et/ou de dynamique de vie familiale des usagers* »¹⁵³. Ce courant sociologique mêle lui aussi théorie informationnelle et pragmatisme en ramenant l'information à un usage, lui-même défini comme une « pratique ». De la même manière que M.-A. Frison Roche associait un mode d'appropriation matérielle (information comme bien) à une activité (l'exploitation de données), les sociologues des usages associent un mode d'appropriation immatérielle (information comme communication) à une activité (l'usage). Ce prisme d'analyse sociologique mène généralement à une même observation empirique : l'objet conditionne l'usage, et l'usage oriente, « norme » la société humaine autant qu'il en provient. Concrètement, Françoise Paquien séguy remarque que

dans une même Constitution (nationale) : v. CHALLE Édouard, « Jürgen Habermas et le fondement communicationnel du droit », *Le Philosophoire*, n° 9, 1999, p. 175-199 ; DESCOMBES Vincent, « Le contrat social de Jürgen Habermas », *Le Débat*, n° 104, 1999, p. 37-44

149HÉRAN François, « La sociabilité, une pratique culturelle », *Économie et statistique*, n° 216, 1988, p. 14

150La distinction liens forts/faibles provient de GRANOVETTER Mark S., « The Strength of Weak Ties », *American Journal of Sociology*, vol. 78, 1973, p. 1360-1380

151DANG NGUYEN Godefroy et LETHIAIS Virginie, « Impact des réseaux sociaux sur la sociabilité. Le cas de Facebook », *Réseaux*, n° 195, 2016, p. 181

152GEORGE Éric, « L'étude des usages des TIC au prisme de la recherche critique en communication » in VIDAL Geneviève (dir.), *La sociologie des usages. Continuités et transformations*, Lavoisier, 2012, v. p. 30-33

153PROULX Serge, « Les différentes problématiques de l'usage et de l'utilisateur » cité par *ibid.*, p. 31

le pouvoir de l'utilisateur, s'il a été accru par « *l'omniprésence d'Internet [qui] a renforcé la « capacité communicative humaine* », s'est par-là même vastement aliéné à l'offre matérielle ou logicielle (activité) d'un objet conçu selon des intérêts économiques. Les usages seraient alors primitivement « *prescrits* » par le concepteur de l'objet¹⁵⁴. Parmi les moyens dont dispose le concepteur pour prescrire l'usage, ont pu être identifiés (i) le *design* de l'objet, qui délimite la capacité de l'utilisateur à effectuer des tâches et derrière lequel on trouve « *ingénieurs, ergonomes, psychologues, philosophes et sociologues, linguistes dont l'objectif consiste à stimuler les affinités entre les usages des TICs et l'interactivité (...) sur la base de modèles cognitifs* »¹⁵⁵; (ii) l'algorithme de l'objet, qui régleme son fonctionnement et oriente les habitudes et parcours numériques des utilisateurs¹⁵⁶ ; (iii) ou encore la structure du réseau qui réorganise les possibilités et modes de communication¹⁵⁷.

S'il est un prescripteur primaire, le concepteur de l'objet n'est pas le seul à remanier les comportements. Par la création de deux comptes Facebook distincts aux comportements sociaux contraires, Antonio Casilli compare méthodiquement les réactions des cercles d'amis entourant respectivement chacun des deux comptes. Le comportement socialement dynamique du premier compte (publications de photos, de goûts musicaux, littéraires...) incitera les 14 membres de son cercle d'amis à s'interrelier par des demandes d'ajouts mutuelles, tandis que le comportement socialement statique du deuxième compte (rares publications de courts messages) n'induit aucune inter-liaison parmi les 14 membres de son cercle d'amis¹⁵⁸. Par ses usages et au moyen de l'objet « réseau social », l'utilisateur est capable de modifier les usages des autres utilisateurs. Ainsi la sociologie des usages est-elle parvenue à démontrer **l'existence d'un lien causal entre la communication en ligne et les comportements sociaux** à travers la « *configuration de l'usager* »¹⁵⁹ par l'objet technologique et ses usages.

En infusant la mécanique sociale *via* la communication, les données en ligne peuvent être saisies à long terme par la compréhension humaine, contribuer aux significations et mouvements de la société. Ce que connaît le droit positif de la liberté d'expression a le mérite de s'appliquer commodément à de telles conclusions. Depuis sa jurisprudence *Handyside* de 1976, la Cour européenne des droits de l'Homme (Cour EDH) reconnaît les effets évolutifs portés par l'expression auprès de la société en faisant de la liberté d'expression « *l'une des conditions de base pour le progrès des sociétés et pour le développement de chaque individu* ». ¹⁶⁰

154PAQUIENSÉGUY Françoise, « L'utilisateur/consommateur producteur de richesse » in AGOSTINELLI Serge, AUGÉY Dominique et LAURIE Frédéric (dir.), *La richesse des réseaux numériques*, Presses Universitaires d'Aix-Marseille, 2012, p. 230-236

155Existerait une « *institution du design informatique* » (PAPILLOU Christian, « L'interactivité. Le défi d'une sociologie des usages des TICs » in VIDAL G. (dir.), *La sociologie des usages*, préc., Lavoisier, 2012, p. 90-117)

156SILVA MOTA DRUMOND Gabrielle, COUTANT Alexandre, MILLERAND Florence, « La production de l'utilisateur par les algorithmes de Netflix », *Les Enjeux de l'information et de la communication*, n° 19/2, 2018, p. 29-44

157MUSIANI Francesca, *Nains sans géants : architecture décentralisée et services Internet*, Presses de l'École des mines, Paris, 2013

158CASILLI Antonio, « Être présent en ligne : culture et structure des réseaux sociaux d'Internet », *Idées économiques et sociales*, n° 169, 2012, p. 16-29

159PROULX Serge, « La sociologie des usages, et après ? », *Revue Française des Sciences de l'information et de la communication*, n° 6, 2015 (au 4^e niveau d'analyse de la deuxième topique de la sociologie des usages)

¹⁶⁰ Cour EDH, *Handyside*, 7 déc. 1976, n° 5493/72, §49

Contrairement par exemple au droit de propriété privée qui a pour objet de préserver un état, la liberté d'expression vise à assurer l'évolution de cet état. Et, à rebours du droit à la vie, la liberté d'expression n'est pas une liberté ou un droit qui introduit l'existence des autres ; c'est une liberté sans laquelle l'humanité est condamnée à stagner. En France, la même solution est retenue par le Conseil constitutionnel, remémorant fréquemment que la liberté d'expression doit adapter sa protection « *en l'état actuel des moyens de communication* »¹⁶¹. La liberté d'expression y a en effet, dès son éclosion, été garantie indifféremment du moyen de communication. L'article 11 de la Déclaration des droits de l'Homme et du citoyen préserve la liberté d'expression quelle que soit la provenance de la communication (issue de capacités corporelles humaines – parler/écrire – ou augmentées par la machine – imprimer), quelle que soit l'ancienneté des moyens avec lesquels s'exprime cette communication. Cette absence de hiérarchisation selon les origines matérielle de la communication ou chronologique de son moyen est confirmée par la loi du 29 juillet 1881 sur la liberté de la presse, dont l'art. 1^{er} insère la librairie dans le champ d'application de la liberté d'expression. En suivant cette continuité, toute étape communicationnelle dans l'histoire de l'humanité est appelée à recevoir le bénéfice de la liberté d'expression indistinctement du support du message (parole, écriture, imprimerie, librairie...) et ainsi accompagner le « *développement* » de la société – pour reprendre les termes de l'arrêt *Handyside*.

Saisir internet sous ses conséquences socio-communicationnelles rend possible son appréhension juridique au titre de la liberté d'expression, aussi bien lorsqu'est impliquée une compréhension humaine à long terme (adaptation de la liberté d'expression aux nouveaux moyens de communication y inclus internet) que lorsqu'est impliquée une compréhension humaine instantanée de l'information en ligne. Cette compréhension à court terme naît de ce que le droit juge généralement comme étant un « contenu » produit ou consulté par l'utilisateur. En France, l'essor de ce concept en 2004 tient fort logiquement la liberté d'expression pour socle : à compter de 1986, la loi Léotard consacre la « liberté de *communiquer* par voie *électronique* »¹⁶² en son article 1^{er} et, ce faisant, définit la « *communication électronique* »¹⁶³ en ciblant les critères de « *l'émission, la transmission ou la réception* » d'un signal électrique. En 2004, le législateur n'entend plus seulement garantir le transport électronique, mais l'*expression* électroniquement transportée. La LCEN distingue deux types de communications électroniques, dont les critères de transport cèdent leur place à des critères tenant au mode de communication : la communication électronique est une « *communication au public en ligne* » (CAPEL) si elle résulte d'une demande individuelle ; c'est une « *communication audiovisuelle* » dans le cas contraire¹⁶⁴. D'après le législateur, il y a demande individuelle si l'utilisateur est capable de produire un contenu, à l'inverse de l'usager de l'audiovisuel qui se contenterait de

161CC, *Loi modifiant la loi du 30 sept. 1986 relative à la liberté de communication*, 17 janv. 1989, n° 88-248 DC, cons. 26 ; CC, *Hadopi I*, 10 juin 2009, n° 2009-580 DC, cons. 12

162À l'époque, « liberté d'installer, d'exploiter et d'utiliser des services de télécommunications », art. 1^{er}, Loi n° 86-1067 du 30 sept. 1986 relative à la liberté de communication. En 1986, il s'agissait surtout d'inscrire dans la loi l'interdiction faite à l'Etat, par respect pour cette liberté, d'exercer un monopole dans l'audiovisuel (TV/ radio) et marquer ainsi au fer législatif la libéralisation décidée 4 ans plus tôt, ouvrant à des personnes privées indépendantes de l'Etat la possibilité d'utiliser des fréquences radioélectriques sur autorisation de la Haute autorité de la communication audiovisuelle désormais Conseil supérieur de l'audiovisuel (« *légalisation des radios-pirates* » par la loi « Fillioud » n° 82-652 du 29 juil. 1982 sur la communication audiovisuelle).

163À l'époque, « *télécommunication* », art. 2 de la même loi

164LCEN, art. 1, IV

« choisir » un contenu préparé par autrui et qui « arrive » à lui¹⁶⁵. Les « contenus en ligne », ou CAPEL, surgissent d' « échanges bidirectionnels »¹⁶⁶ (l'émetteur et le récepteur peuvent interchanger leurs rôles) contrairement aux contenus audiovisuels qui s'inscrivent dans une relation unidirectionnelle (le récepteur ne peut émettre).

La régulation d'internet par les contenus n'était pas privilégiée, le législateur de 2004 n'ayant énoncé que trois types de contenus contre lesquels les opérateurs et hébergeurs devaient activement concourir à la lutte en les retirant « promptement » une fois signalés (apologies d'actes de terrorisme et de crime contre l'humanité, pédopornographie, incitation à la haine raciale (art. 6, I, 7 LCEN)). En revanche, l'emprise de la liberté d'expression sur internet a très tôt été totale car, sous cet angle informationnel, toute donnée produite en ligne ou presque constitue une communication. Ainsi, tout en érigeant l'existence d'une « liberté d'accès aux services de communications au public en ligne [CAPEL] », le Conseil constitutionnel refuse catégoriquement d'en faire une liberté autonome de la liberté d'expression¹⁶⁷. Cette application totaliste de la liberté d'expression à internet se lit aussi dans la jurisprudence de la Cour EDH. Après avoir vu dans les sites internet une fonction « facilitatrice [pour] la communication de l'information » du fait de leur « capacité à conserver de grandes quantités de données »¹⁶⁸, elle finit par rendre la liberté d'expression applicable à internet *en tant qu'il constitue un moyen de communication* dont tout acteur peut prétendre au bénéfice (y compris les plateformes d'hébergement pour se voir appliquer le droit de la presse)¹⁶⁹, « quel que soit le type de message et même lorsque l'objectif poursuivi est de nature lucrative »¹⁷⁰. Juridiquement, la communication est essentielle à internet : la propriété intellectuelle vaut certes pour certaines données « originales », la cybersécurité pour les cyberattaques, la protection des données personnelles pour celles identifiantes... mais la liberté d'expression, elle, s'applique à toutes les données en ligne.

En conclusion, des scientifiques d'internet ainsi que des ordres juridiques semblent avoir adopté une conception exogène du réseau : animé par des objets ou des sujets qui lui sont extérieurs, le réseau est régulé par le biais de machines ou d'acteurs humains qui en ont fait une appropriation pratique ou informationnelle. Cette conception dominante dans les discours scientifique et étatique n'est pas exclusive d'une approche plus endogène d'internet, alors conçu comme un réseau impulsé par une vie propre.

165Assemblée Nationale, Rapport législatif n° 612 [*supra* note], 2003, p. 13

166Ibid., p. 35

167CC, Commentaire de la décision n° 2009-580 DC [Hadopi 1], p. 6-7 : « le Conseil a jugé que le droit de se connecter à internet relève de l'exercice de la liberté de communication et d'expression. Internet peut également constituer un outil professionnel permettant l'exercice de la liberté du commerce et de l'industrie, mais, fondamentalement, au-delà des usages qu'il peut en être fait, il est d'abord un moyen de communication. C'est donc à l'exercice de la liberté énoncée à l'article 11 de la Déclaration de 1789 que le Conseil s'est référé. (...) Compte tenu du rôle que joue internet dans l'accès à l'information, la protection constitutionnelle de la liberté de communication et d'expression, s'applique également à internet. (...) le Conseil n'a pas seulement affirmé que l'accès à internet entre dans le champ du droit constitutionnel de s'exprimer et de communiquer librement. Il a jugé que ce droit implique [souligné par le CC] la liberté d'accéder à internet. ».

168Cour EDH, 4^e sect., *Times Newspapers Ltd c. Royaume-Uni* (n^{os} 1 et 2), 10 mars 2009, n° 3002/03 et 23676/03, §27

169Cour EDH, Gde ch., *Delfi AS c. Estonie*, 16 juin 2015, n° 64569/09, v. notam. §110

170Cour EDH, 5^e sect., *Ashby Donald e. a. c. France*, 10 janv. 2013, n° 36769/08, §34

Chapitre 2. La conception endogène du réseau internet

L'acteur d'internet est parfois tenu pour indivisible du réseau. Dans ce cas, les deux forment une unité propre, comme si l'acteur-réseau était distinct de l'acteur-urbain. L'acteur-réseau et l'acteur-urbain appartiendraient à deux mondes autarciques régis par leurs normativités respectives. À la manière d'un « cyberspace », le réseau internet admettrait en son sein des normes qui en détermineraient l'agencement (Section 1). Lorsqu'elle est enrichie par les leçons tirées de la conception exogène, celle endogène discerne plusieurs foyers de normativité qui, croisés voire cumulés, renforceraient le pouvoir normatif de certains acteurs en ligne par rapport à d'autres (Section 2).

Section 1. Une normativité issue d'un « cyberspace »

Après que des scientifiques aient observé l'existence d'une « vie » normative interne à la Machine indétachable de l'humanité (Paragraphe 1), il put en être fait application au cyberspace (Paragraphe 2).

Paragraphe 1 - L'absorption de l'être humain dans une normativité machinale

Les premières réflexions portant sur l'autonomie de la Machine (A) ont été enrichies par les approfondissements d'une fusion Homme-Machine révélant la normativité de cette relation (B).

A) L'autonomie de la Machine

Jusqu'aux années 1950, l'objet technique était philosophiquement appréhendé dans son contexte spatio-temporel. Platon invitait les êtres humains à ne pas abandonner leur mémoire aux livres, à soigner leur faculté de retenir ce que l'écrit ne fige pas, pour sauver leur indépendance d'esprit¹⁷¹ ; pour René Descartes, la science et ses résultats physiques représentent la capacité de l'Homme à dominer la Nature par la connaissance¹⁷² ; quant à Martin Heidegger, il opinait dans cette droite ligne que, par la Technique, « *la nature est mise en demeure de livrer une énergie* »¹⁷³ dont la diffusion modifie le rapport entre l'être humain et son cadre de vie, donc sa pensée. La Technique est examinée dans ses répercussions sur la mémoire humaine, sur l'environnement humain ou encore sur les conditions de l'existence humaine. On ne saurait synthétiser en quelques lignes toute la réflexion philosophique menée sur la Technique jusqu'au XXe siècle, mais c'est depuis le milieu du XXe siècle que les « philosophes de la Technique » isolent l'objet technique de son contexte. Plus précisément, l'objet technique est regardé comme « autonome ».

Dans sa thèse de doctorat publiée en 1958, Gilbert Simondon traite l'objet technique à l'instar d'un système. Repérable par la cohérence de son fonctionnement interne, l'objet technique fournit des fonctions qui s'assemblent ou s'articulent à l'intérieur d'un même objet, ainsi qualifié de « technique » par G. Simondon¹⁷⁴. Prises isolément, ces fonctions représenteraient l'« élément technique » de l'objet, et leur assemblage/articulation

171STIEGLER Bernard, *Pour une nouvelle critique de l'économie politique*, Galilée, 2009, p. 43s (v. les 7 et 8)

172DESCARTES René, *Discours de la méthode*, Cinquième partie, p. 308 [en ligne]

173BOUTOT Alain, *Heidegger*, PUF – Coll. *Que sais-je ?*, 1995, p. 88

174SIMONDON Gilbert, *Du mode d'existence des objets techniques*, 2012, Aubier, p. 24s.

formeraient l' « individu technique » de l'objet qui permet généralement de l'identifier visuellement ou lexicalement¹⁷⁵ . Les interactions de l'élément technique avec son niveau supérieur, l'individu technique, provoqueraient une réalité interne à l'objet technique qui n'est connue ni de l'être humain (milieu humain), ni du contexte de l'objet (milieu contextuel), mais du seul objet lui-même (« *milieu assimilé* »¹⁷⁶). Ne jouent, à l'intérieur de l'objet, que ses règles de fonctionnement.

Ces analyses rappellent celles de l'ethnologue et archéologue André Leroi-Gourhan, inspectant lui aussi la Technique par la notion de « milieu ». Dès 1945, A. Leroi-Gourhan départage un « *milieu intérieur* » (i.e. la composition d'un objet technique tels les atomes d'un microphone), un « *milieu extérieur* » (i.e. l'environnement dans lequel l'objet prend place telle la présence d'un être humain à proximité du microphone) et, entre les deux, un « *milieu technique* ». Ce milieu technique regroupe toutes les fonctions grâce auxquelles le milieu intérieur d'un objet peut entrer en communication avec son milieu extérieur (par ex., l'ouïe fait partie du milieu technique grâce auquel le son reproduit par le micro peut entrer en communication avec l'être humain). Au contact de ce troisième milieu, de cette « technosphère »¹⁷⁷, l'objet deviendrait capable d'étendre son effet au-delà de son milieu interne. L'évolution d'un objet technique s'expliquerait alors par l'existence du milieu technique qui permet au développement de l'objet de ne plus être immobilisé par sa composition, de s'en extraire auprès de l'extérieur. En d'autres termes, plus ce milieu technique s'enrichit, plus les objets techniques se sophistiquent et inversement.

Appliquons cette théorie à l'objet « réseau électrique » : son existence prend pied à la fois dans un milieu intérieur (les machines membres du réseau) et dans un milieu extérieur (environnement naturel ou artificiel, émetteur/récepteur humain...) reliés par un milieu technique (fonctions de transport de signaux électriques). L'absence d'un milieu technique (transport) empêcherait l'objet d'évoluer car il ne pourrait accéder au milieu extérieur qui lui offre son développement. Mais sa présence rend le milieu intérieur accessible au milieu extérieur : (i) la mise en contact réseau/Nature *via* le transport révèle des bruits de fond ; (ii) la mise en contact réseau/humain *via* le transport ouvre la possibilité d'expérimenter humainement l'objet réseau pour en résorber les bruits de fond. Le réseau analogique a ainsi pu évoluer au profit du réseau numérique. Du réseau télégraphique à internet, chaque étape franchie est le fait de mises en relation successives entre le milieu intérieur de l'objet et son milieu technique (transport), puis entre son milieu technique et son milieu extérieur, puis entre son milieu extérieur et son milieu intérieur. Au cours de cette évolution, si la composition de l'objet se sophistique, son milieu technique s'enrichit à son tour : les paquets IP ne sont pas transportés comme l'étaient les télégraphes. Ce milieu *technique* connaît un enrichissement, un développement qui lui est spécifique, qui se situe en- dehors des deux autres milieux et qu'A. Leroi-Gourhan baptise « évolution *technique* ». L'évolution technique suivrait alors un rythme propre, certes impulsé de l'extérieur mais non-

175 Cette distinction élément/individu techniques qui nous semble très pertinente pour synthétiser le propos de G. Simondon ne nous vient pas du philosophe lui-même mais d'un commentateur-blogueur : « Du mode d'existence des objets techniques de Gilbert Simondon », 2017 [en ligne sur quaternum.net]

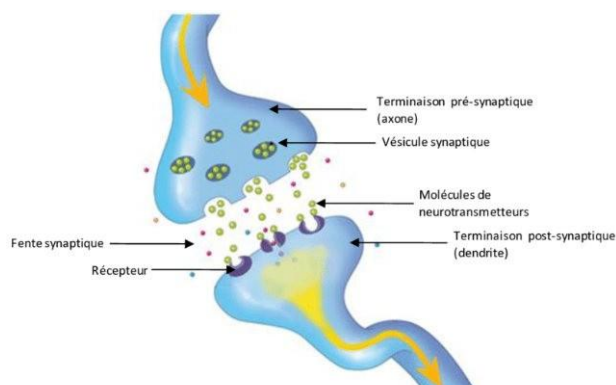
176 SIMONDON G., *Du mode d'existence des objets techniques*, préc., p. 70

177 Entre « biosphère » et « noosphère » : POPLIN François, « André Leroi-Gourhan et le monde animal » in Collectif CNRS., *André Leroi-Gourhan ou les Voies de l'Homme*, Actes du colloque du CNRS (mars 1987), Albin Michel, 1988, p. 54

aligné sur les règles des deux autres milieux¹⁷⁸. L'archéologue y fait correspondre une « *biologie de la technique* » séparée de la biologie organique humaine, par laquelle il justifie le différentiel entre les dynamiques évolutives de ces deux biologies – ce qui lui vaudra la critique de bloquer l'étude humaine d'une évolution technique connue du seul milieu technique¹⁷⁹. Un demi-siècle plus tard, l'astrophysicien Stephen Hawking prédit que « *les humains, limités par une lente évolution biologique, ne pourraient pas rivaliser et seraient supplantés* » par l'intelligence artificielle (IA), dont l'évolution non bornée par les mêmes lois biologiques rattraperait progressivement celle des êtres humains pour la dépasser¹⁸⁰.

Quittant la métaphore du « milieu », des ingénieurs et psychologues interrogeaient moins l'autonomie préexistante de l'objet technique que l'autonomie pouvant être techniquement octroyée à un objet initialement incapable de penser. Nourrissant le rêve d'une machine apte à raisonner, les ingénieurs John McCarthy¹⁸¹, Marvin Minsky, Nathaniel Rochester et Claude Shannon déposent auprès de l'Université de Dartmouth une « *proposition pour un projet de recherche sur l'Intelligence Artificielle* » en 1955. Cette *intelligence est artificielle* parce qu'elle correspond à la *simulation* d'un « *réseau neuronal* » défini comme « *la manière dont un ensemble de neurones (hypothétiques) peut être disposé de manière à former des concepts* »¹⁸². Deux ans plus tard, le psychologue Frank Rosenblatt conçoit pour le laboratoire d'aéronautique de l'université Cornell un modèle théorique de connexions neuronales – le perceptron.

Cet algorithme s'appuie sur les connaissances neurologiques déjà établies : lorsque le cerveau humain doit traiter une information, cette dernière est d'abord stockée dans les vésicules synaptiques qui composent la « terminaison pré-synaptique » d'un neurone ; cette



Extrait de Anne Meunier, *Méthodes analytiques pour la détection de phénomènes biologiques de sécrétion l'échelle de la cellule unique*, 2011, p. 32 [en ligne sur [researchgate.net](https://www.researchgate.net)]

activité de stockage amène le neurone pré-synaptique à libérer des neurotransmetteurs, molécules qui transmettent l'information aux récepteurs du neurone post-synaptique. La connexion interneuronale est donc caractérisée par au moins deux couches: une couche d'entrée qui récupère l'information, et une couche de sortie qui apporte une réponse à l'information communiquée. D'où il devient possible de connaître le « *poids synaptique* » d'une relation entre deux

178GRANAI George, « André Leroi-Gourhan, A. - Evolution et techniques. Vol. I : L'homme et la matière ; Vol. II : Milieu et techniques ; B. - Archéologie du Pacifique nord » in *Revue de géographie de Lyon*, vol. 26, n°4, 1951, p. 461 : « *les faits techniques sont appréhendés dans un milieu abstrait, immobiles, et sans rapports avec ce qui est en deçà et ce qui est au-delà de cette "zone moyenne" qu'éclaire l'Histoire* »

179Sur ces critiques et leur relativisation, v. GUCHET Xavier, « Evolution technique et objectivité technique chez Leroi-Gourhan et Simondon » [sur *Open Edition*], *Appareil*, n° 2, 2008

180« Stephen Hawking warns artificial intelligence could end mankind » [en ligne], *BBC*, 2014

181On notera au passage que John McCarthy (Professeur au MIT de 1956-1962) co-initiera en 1963 le premier projet d'un réseau électrique faisant communiquer concomitamment des dizaines de terminaux (projet *Multiple Access Computer* prédécesseur d'ARPANET)

182MCCARTHY John, MINSKY Marvin, ROCHESTER Nathaniel et SHANNON Claude, *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 31 août 1955, pt. 3 (publié par *AI Magazine*, vol. 27, 2006)

neurones, c'est-à-dire son influence dans un réseau de neurones, en connaissant la mesure dans laquelle l'élément post-synaptique peut répondre à l'entrée venant de l'élément pré-synaptique. Cette mesure, calculée par un « *coefficient synaptique* », dépend d'un seuil¹⁸³ au-delà duquel le neurone post-synaptique peut fournir une réponse (le neurone ne réagit pas à un signal linéaire, continu, mais au dépassement d'un seuil avec lequel coïncide une fonction mathématique dite « non linéaire »). Dans ces conditions, une variation du coefficient synaptique, du seuil de chaque neurone ou encore de la structure du réseau neuronal entraîne une variation des poids synaptiques en présence. Sur cette base, le neuropsychologue Donald Hebb établira des associations entre des coefficients synaptiques et les activités précisément correspondantes des unités reliées. Avec son perceptron, F. Rosenblatt intègre ces associations (« loi de Hebb ») dans un algorithme de calcul valable à l'échelle d'un réseau neuronal. À l'origine composé de deux couches (entrée/sortie), ce réseau neuronal se complexifiera à travers les avancées scientifiques. Le perceptron multicouche en est un exemple : en plus des couches d'entrée et de sortie, il comporte « *une ou plusieurs couches cachées* » dans lesquelles « *il suffit d'ajouter un nombre de neurones suffisant pour approximer n'importe quelle fonction non linéaire* »¹⁸⁴ et ajuster ainsi les résultats produits par le réseau neuronal.

Cette intelligence artificielle (IA) dite « connectée », car assise sur l'inter-liaison d'unités, fut toutefois arrêtée dans ses progrès au début des années 1960, après que M. Minsky a soulevé l'impossibilité technologique de programmer un logiciel capable de résoudre des problèmes non-linéaires. Le constat fit abandonner la piste connectée au bénéfice d'une IA dite « symbolique », bâtie non plus sur des inter-liaisons mais sur des théorèmes, sur l'élaboration d'étapes didactiques à suivre dans le but de résoudre un problème. Ce fut là toute l'œuvre de l'économiste et sociologue Herbert Simon. Révisant la « rationalité instrumentale » wébérienne – pour Max Weber, les agissements économiques de chacun seraient orientés par l'organisation culturelle d'appartenance des agents (capitalisme, religion...), intégrant ainsi leur Raison comportementale – H. Simon estime que cette rationalité instrumentale est « *limitée* » : bien qu'objective, l'organisation culturelle est reçue par l'agent dans la limite de ses capacités cognitives subjectives. Pour conclure au caractère limité de ces capacités cognitives, H. Simon considère que le raisonnement humain hiérarchise des questionnements élémentaires (et non infinis), respectant une « *procédure* » d'opérations séquentielles¹⁸⁵. Hachant méthodiquement cette rationalité procédurale en plusieurs paliers d'un raisonnement automatisable, il co-réalisa en 1959 avec l'ingénieur Allen Newell le premier solveur universel (*General Problem Solver*), un programme informatique théoriquement capable de résoudre n'importe quel problème qui lui est soumis. La logique déductive de ce programme n'est toutefois valable que pour un problème immobile, dont les données n'évoluent pas. Pour traiter des problèmes évolutifs, il a fallu adopter une logique « non-monotone »¹⁸⁶ qui ajoute à la connaissance du programme de nouveaux faits sans en retirer les faits antérieurs. Nonobstant son évolution, le problème peut ainsi être résolu par accumulation de connaissances.

183Correspondant à une valeur w_0 issue des travaux de formalisation d'un neurone des neurologues MCCULLOCH Warren S. et PITTS Walter, « A logical calculus of the ideas immanent in nervous activity », *The bulletin of mathematical biophysics*, vol. 5, 1943, p. 115-133

184CHRAIBI KAADOUD Ikram et GARENNE André, « Architecture des réseaux de neurones: Réseaux de neurones artificiels classiques (2/3) ! », sur *Scilogs.fr*, 2018

185SIMON Herbert, *Administrative Behavior*, Macmillan, 1947

186Le langage de programmation *ProLog* développé en 1972 en est l'une des premières applications

Seulement les progrès de l'IA symbolique ralentissent depuis les années 2000 face à la recrudescence de l'IA connectée. Au début du 3^e millénaire, les obstacles techniques soulignés par M. Minsky n'étaient plus d'actualité : le perceptron de F. Rosenblatt est devenu technologiquement faisable. Le *Deep Learning* reproduit ainsi un réseau neuronal pour rendre possible la prise de décision tandis que le *Machine Learning*, second courant dominant de l'IA connectée moderne, emploie des algorithmes mettant en relation une grande quantité de données pour en inférer des conclusions.

En résumé, les réflexions et travaux présentés entrevoient une autonomie dans l'objet technique. Qu'elle soit de fonctionnement (autorégulation de G. Simondon), d'évolution (biologie technique de A. Leroi-Gourhan) ou de raisonnement (IA), cette autonomie est la conséquence d'une séparation Homme/Machine : la Machine est autonome en tant qu'elle possède une existence, une « vie » déprise de la vie humaine ; elle intègre un milieu (« *assimilé* » ou « *technique* ») inoccupé par l'être humain, ou elle est pourvue d'un processus décisionnel à l'issue incontrôlable par l'être humain. Ces discours et expérimentations apportent donc les prémices d'une analyse « endogène » de l'objet technique isolé de son contexte, mais ne font pas fusionner l'être humain et la Machine.

B) La fusion normative de l'Homme et de la Machine

On a déjà défini en Introduction la « norme » comme « la signification d'un devoir-être ». Par « normativité », on désignera le phénomène par lequel un devoir-être est signifié. En ce sens, une fusion normative de l'Homme et de la Machine renvoie à la double hypothèse d'un devoir-être signifié à l'Homme par la Machine et d'un devoir-être signifié à la Machine par l'Homme, de telle manière que l'Homme et la Machine s'influenceraient mutuellement sur le plan normatif.

En maintenant le clivage Homme/Machine, les premières études sur l'autonomie de l'objet technique situaient nécessairement la normativité humaine *en-dehors* de la Machine. Certes, le philosophe G. Simondon n'excluait pas que la réalité interne à l'objet technique puisse véhiculer des « *aspects normatifs* » (« *culturels, esthétiques voire moraux* ») ; cependant, cette réalité interne n'est pas normative en elle-même¹⁸⁷. La normativité est extérieure à cette réalité interne, provient de l'être humain qui reste maître de la Machine. Cette domination normative de l'être humain sur la Machine recoupe le pouvoir du « technicien ajusteur » décortiqué par le sociologue Michel Crozier. Expérimentant le fonctionnement d'un organisme industriel d'État, M. Crozier constate que, du technicien qui répare les machines, dépendent à la fois les ouvriers qui les utilisent et le directeur qui ne peut plus faire tourner l'atelier en cas de panne. En tant qu'il exerce le pouvoir sur la Machine dont dépend l'atelier, le technicien représente structurellement la première source de pouvoir dans l'atelier¹⁸⁸. L'une des leçons pouvant être

187Entretien de Gilbert Simondon avec le journaliste Yves Deforges, de 1min 35s à 4min 10s dans la 2^e partie « Rapports » du film *Le point sur la technologie* réalisé par Jacques Jahan en 1967 pour la TV scolaire [en ligne sur cndp.fr]

188Dans les faits, le technicien ne peut toutefois exercer librement son pouvoir que dans un faible périmètre (celui de ses tâches, de ses *opérations* individuelles) mais « *perd son droit de veto* » lorsque sont fixés de larges programmes d'action qui concernent collectivement l'atelier et qui placent le directeur dans une situation « *coopérative* », impliquée dans les tâches du technicien sur lequel il exerce une autorité hiérarchique de fait : CROZIER Michel, *Le phénomène bureaucratique*, Seuil, 1963, p. 180

tirées de cet examen empirique est l'apport d'une démonstration concrète qu'une société déterminée peut dépendre du fonctionnement d'une Machine.

De ces mêmes fondements, les penseurs d'une fusion Homme-Machine, d'une part, ont abandonné l'idée que la Machine serait séparable de l'être humain : si l'activité d'une société humaine dépend d'une Machine, et si une Machine contient une réalité autonome, alors ladite activité humaine peut dépendre de la réalité autonome de la Machine. D'autre part, ils ont renversé l'argumentation sur l'autonomie de l'objet technique : si la Machine doit son autonomie à des règles intrinsèques, l'activité humaine qui en dépend incorpore ces règles dans son fonctionnement. **Par « fusion Homme-Machine », on visera donc le phénomène qui ferait de l'être humain urbanisé obéissant à des lois urbaines voire naturelles un être humain technologisé obéissant aux lois internes de la Machine.** La normativité humaine est intégrée dans la Machine autant que la Machine devient en elle-même normative pour l'être humain. Parmi les premières problématiques suggérées par ces horizons nouveaux, celle tenant à savoir si la fusion normative en cause est libératrice ou aliénante pour l'être humain.

Elle est regardée comme « libératrice » lorsqu'elle contribue à l'épanouissement de l'être humain ou de la société humaine. Avant que se consolide une conception endogène claire, les théories cybernétiques de N. Wiener positionnaient certes l'être humain à l'extérieur de la Machine mais annonçaient (et militaient pour) une fusion des deux. Pour rappel [*supra*], N. Wiener oppose l'entropie (manifestée par le bruit) et l'information (qui insère de la forme là où il y a du chahut, du chaos). L'un des principes fondamentaux de la cybernétique en découle : plutôt que de tracer une frontière infranchissable entre l'Homme et la Machine comme c'était la tendance de son époque, il invite à les réunir ; porteuse d'informations, la Machine pourrait corriger les aléas humains (émotions politiques, économiques...) générateurs d'entropie. Plus la société se technologise, plus elle produit d'informations en sorte que, prédit-il, il sera bientôt impossible de comprendre la société sans la connaissance de ces informations et de leur fonctionnement technique¹⁸⁹ ; l'être humain ne pourra plus se passer de la Machine pour informer la société et en éliminer les désordres. L'avenir souhaité par le mathématicien américain est celui d'une société humaine guidée par l'information, dont la domination sur l'Homme supplanterait la domination de l'Homme sur l'Homme. L'appropriation de l'information étant écartée par la cohérence cybernétique – car génératrice d'entropie –, l'être humain se retrouverait dominé par une rationalité autorégulée dont la Machine est la gardienne.

L'approfondissement d'une conception endogène de l'objet technique à partir de la fin des années 1950 (en philosophie, ethnologie/archéologie, ingénierie/psychologie, biologie...) a croisé la théorie cybernétique pour, nous semble-t-il, attiser le renouvellement du transhumanisme depuis les années 1970. Dans sa première ère entamée à la fin du XVIIIe siècle, le transhumanisme est rétroactivement rapporté à des figures comme Nicolas de Condorcet ou Benjamin Franklin¹⁹⁰. Inspiré par la mécanique de Jacques Vaucanson, N. de Condorcet fantasme d'un Roi « automate » résumé à la fonction de ritualiser la Nation¹⁹¹ et d'un citoyen instruit pour exercer

189WIENER Norbert, *The human use of human beings : cybernetics and society*, Houghton Mifflin, 1954, p. 48

190DAMOUR Franck, « Le mouvement transhumaniste. Approches historiques d'une utopie technologique contemporaine », *Vingtième Siècle. Revue d'Histoire*, n° 138, 2018, p. 143-156

191 DE CONDORCET Nicolas, *Lettres d'un jeune mécanicien aux auteurs du Républicain*, 1791

pleinement sa Raison¹⁹². Inspiré par les lois électriques et la compréhension scientifique du monde, B. Franklin misait sur la plus large diffusion possible de la science à travers ses librairies, comptait parmi les premiers instigateurs d'une politique démographique quantifiée¹⁹³ et calculait la pertinence d'une décision politique selon un bilan coût-avantage à partir des données de son époque¹⁹⁴.

Il y a, chez ces deux penseurs, une part politique et une part technique. La part politique¹⁹⁵ : tous deux envisagent le progrès de la société humaine à travers le contrôle rationalisé de la Nature par l'être humain, quand d'autres forces politiques « réactionnaires » appellent à préserver la Nature de l'instrumentalisation humaine (le romantisme auquel succéderont les « bioconservateurs » tels le *New Age*, l'écologie profonde, les altermondialistes). La part technique : les deux aspirent au prolongement de la vie humaine, N. de Condorcet par la voie médicale et B. Franklin par une « *méthode d'embaumement* » qui donnerait la possibilité de réveiller une personne un siècle après son trépas¹⁹⁶. Cet espoir fut scientifié par l'universitaire Robert Ettinger qui, en 1962¹⁹⁷, conçoit la faisabilité d'une cryonie humaine dans le but de ramener un être humain à la vie au moment choisi après l'avoir provisoirement éteinte, tout en préservant l'intégrité du corps humain le temps de cette éteinte. La première cryogénisation opéra en 1967 sur la personne du psychologue James Bedford. Persuadé de l'avenir scientifique d'une jeunesse éternelle, épluchant les « *déficiences de l'Homme naturel* »¹⁹⁸, R. Ettinger se revendiquait « *transhumaniste* »¹⁹⁹. Il relaie par là une expression inventée en 1957 par le père de

192KINTZLER Catherine, *Condorcet : L'instruction publique et la naissance du citoyen*, Gallimard, 1987, p. 216s.

193La surpopulation ne dépendrait pas du nombre de personnes membres d'une population, mais de leur « *entassement et interférences avec les autres moyens de subsistance* », règle sur laquelle Thomas Malthus fondera une partie de ses théories économiques : FRANKLIN Benjamin, *Observations Concerning the Increase of Mankind, Peopling of Countries, etc.*, 1751, obs. n° 22

194Pour sortir de la compression entre, d'une part, les menaces séditionnelles de la Ligue des Iroquois et, d'autre part, l'occupation française intimidante de territoires du sous-continent, B. Franklin proposa dans un premier temps, en 1748, des alliances locales avec les Amérindiens « *pour mieux lutter contre les ambitions françaises* » puis dans un second temps, au Congrès d'Albany de 1754, une alliance entre les colonies britanniques (ex-Etats-Unis) pour faire face au « *double péril indien et français* » (LACROIX Jean-Michel, *Histoire des Etats-Unis*, PUF, 2013, p. 58s. et p. 64s.). Les décisions politiques de B. Franklin seraient ainsi moins guidées par des principes idéologiques fixes que par la solution perçue comme la plus adaptée aux circonstances dans l'intérêt des Etats-Unis (HOUSTON Alan, *Benjamin Franklin and the Politics of Improvement*, Yale University Press, 2008)

195Sur les enjeux politiques du transhumanisme, v. DAMOUR Franck, « Le mouvement transhumaniste », préc., *Vingtième Siècle. Revue d'Histoire*, n° 138, 2018, p. 143-156 dont on cite la référence aux « bioconservateurs »

196BOSTROM Nick, « A History of Transhumanist Thought », *Journal of Evolution and Technology*, vol. 14, 2005 [en ligne sur jetpress.org]

197ETTINGER Robert, *The Prospect of Immortality*, 1962 [en ligne sur cryonics.org]

198ETTINGER Robert, *Man into Superman*, 1972, p. 13s. [en ligne sur cryonics.org]

199 *Ibid.*, préface de 1989 par ETTINGER R., p. 4 : « Nous aimons notre corps - lorsqu'il fonctionne - mais il est indéniable que nous sommes faits de matériaux très bon marché. Notre esprit a fait des merveilles, mais il est faible comparé au potentiel que nous entrevoyons. Nos émotions sont souvent délicieuses ou utiles, mais elles sont trop souvent fragiles et erratiques. Certains nous reprochent d'être immortalistes, transhumanistes, et de faire preuve d'orgueil, parce qu'autrefois, il semblait y avoir de bonnes raisons d'accepter ce statut (...) nous ne pouvons pas faire grand-chose à ce sujet (...) la santé mentale et la stabilité de la société pouvaient exiger la résignation. (...) La "condition humaine" (...) est axée sur les limites et les contradictions inhérentes. (...) La condition transhumaine est celle d'une vie illimitée - sans bornes admises dans le temps, l'espace ou la qualité. »

l'eugénisme, Julian Huxley, pour nommer le souhait de voir les facultés humaines améliorées par la science et les technologies²⁰⁰.

À cette première ère transhumaniste qui s'interroge sur la façon de parfaire la vie humaine par la rationalité (eugénistes, immortalistes...) succède, dans les années 1970, une ère qui débat sur la façon dont la société humaine peut évoluer technologiquement. Le débat prend une tournure endogène ; l'amélioration scientifique n'est plus apportée à l'individu humain, mais *par* une société technologisée en son sein. D'un côté, les libertaires extropiens (Max More, FM-2030...) contestent la pertinence de l'entropie pour définir une société humaine : l'intra-destruction d'un système révélatrice d'une entropie ne caractérise pas la société humaine, qui ne cesse d'évoluer sans limites grâce aux sciences et aux technologies. Dans une extropie, le système ne prend alors fin que si cesse l'évolution technologique. De l'autre côté, les « singularistes » estiment au contraire que l'évolution techno-sociale n'est pas continue : les progrès de l'IA aboutiraient à un point de rupture technologique (la « Singularité ») au-delà duquel l'intelligence humaine perdrait le contrôle des technologies et serait dépassée par l'IA, accouchant d'une nouvelle société dont l'être humain ne serait plus la pièce maîtresse²⁰¹. À rebours des extropiens qui militent pour une IA illimitée, ceux qui créditent l'hypothèse de la Singularité mettent l'humanité en garde contre un emballement de l'IA²⁰². Les découvertes techniques encouragent à resserrer les liens de l'Homme et de la Machine. À la fin des années 1970, le transhumaniste Kim Eric Drexler matérialise les premières nanotechnologies qui, entre autres, permettront à tout utilisateur de porter quotidiennement ces technologies sur soi, voire *en soi* comme le propose Elon Musk (transhumaniste aussi) avec sa puce *Neuralink* connectée au cerveau pour transmettre des signaux neurologiques à distance²⁰³. En 2013, la société Google investit 750 millions de dollars dans le projet Calico pour stimuler la recherche sur une ambition immortaliste, par ex. partagée par M. Minsky en 1991 : le téléchargement de l'esprit humain (*Whole Brain Emulation*), sa *transformation* logicielle en bits stockés dans la mémoire d'un ordinateur²⁰⁴. L'Homme n'obéirait plus aux lois humaines, mais à celles définies par la Machine.

Cette fusion normative, contemplée ici comme libératrice, est dénoncée là comme aliénante par le philosophe de la technique Jacques Ellul dès 1954. J. Ellul appuie ses théories sur la *praxis* dans son versant marxiste. Sous cette signification, la *praxis* est le lien qu'entretiendrait

200HUXLEY Julian, *New Bottles for New Wine*, Chatto & Windus, 1957, p. 13-17 (« Transhumanism »)

201La scientificité de la théorie de la singularité est réfutée par de nombreux informaticiens spécialistes de l'IA, au premier rang desquels, en France, GANASCIA Jean-Gabriel, *Le Mythe de la Singularité. Faut-il craindre l'intelligence artificielle ?*, Seuil, 2017

202BOSTROM Nick, *Superintelligence*, Dunod, 2017 (trad. fr. de la version originale de 2016)

203Lancée en 2016 pour permettre de s'exprimer à des personnes qui en sont physiquement incapables, d'augmenter les capacités cérébrales et interactions neuronales, voire de guérir certaines maladies dues à un dérèglement psychique à l'aide d'une correction apportée par le *Neuralink*, cette puce a été employée avec succès sur des cochons en août 2020 : « Elon Musk a testé son implant Neuralink sur des cochons », *Sciences et avenir*, 2020 [en ligne]. En 2018 déjà, le Guardian documentait les récentes évolutions neuroscientifiques des prothèses bioniques en substitut de membres amputés, contrôlées depuis un implant cérébral : « Beyond bionics: how the future of prosthetics is redefining humanity », *The Guardian*, 2018 [en ligne sur YouTube]. À la différence du *Neuralink*, ces implants ne sont toutefois pas contrôlables à distance via un réseau électronique.

204BOSTROM Nick et SANDBERG Anders, *Whole Brain Emulation. A Roadmap*, 2008 [en ligne sur le site du *Future of Humanity Institute* de l'Université d'Oxford]

l'Homme avec la Nature²⁰⁵ et par lequel toute modification de la Nature entraînerait une modification des rapports de production, *i.e.* des relations humaines intermédiées par les biens et services en circulation. Pour le dire autrement, ce que transforment les êtres humains de ce que la Nature leur donne déterminerait les rapports économiques de leur société : par les méthodes d'agriculture, d'élevage et d'artisanat employées, la surproduction romaine requerrait des forces de travail supplémentaires cherchées du côté des prisonniers de guerre, renvoyées vers des tribus non pastorales et divisées (par le travail) des tribus pastorales²⁰⁶ ; par l'industrialisation, le salariat apparut comme nouveau rapport de production ; et par la technologisation, transformation contemporaine de la Nature, la société humaine subirait d'autres bouleversements économiques encore. J. Ellul modernise la théorie marxiste en décrivant ces bouleversements qu'il constate dans son œuvre retentissante sur *La Technique* :

« Ce qui coordonne et rationalise, ce n'est plus l'homme mais les lois internes de la technique ; (...) l'unité intrinsèque de la technique seule assure la cohésion entre les moyens et les actions des hommes ; ce règne lui appartient (...). L'homme est placé devant un choix exclusif, utiliser la technique comme elle doit l'être selon les règles techniques, ou ne pas l'utiliser du tout ; mais impossible de l'utiliser autrement que selon les règles techniques. ».

L'humanité entrerait dans un nouveau rapport de domination, une domination œuvrant au sein du « Système » autonome de la Machine²⁰⁷. Ce « Système » interne à la technique recoupe l'autorégulation simondonienne de l'objet technique en son dedans, à ceci près que G. Simondon n'y faisait correspondre aucune normativité propre. L'aliénation de l'être humain par les lois inhérentes à l'objet technique, telle que la dépeint J. Ellul, signale au contraire l'absorption de l'être humain dans une normativité technique propre à l'objet. Qu'elle soit libératrice ou aliénante, cette fusion normative Homme/Machine a inévitablement attiré les scientifiques du Droit familiers de la normativité qui en ont recherché les implications dans le réseau numérique.

Paragraphe 2 - La vie normative du cyberspace

L'imperméabilité parfois prêtée à internet vis-à-vis de la normativité juridico-étatique (A) a fait voir un cyberspace proprement normatif aux lois duquel seraient soumis ses acteurs (B).

A) L'autarcie normative du réseau

Pour le juriste qui étudie le Droit par le prisme de l'État, une norme/un ordre normatif existe *en soi* si son existence n'est pas tributaire de l'État. Synthétisant les principales dissections théoriques faites de l'ordre juridique, Charles Leben remarque avec beaucoup de hauteur que :

205ELLUL Jacques, *La pensée marxiste*, La Table Ronde, 2003, p. 43

206SAAD Christian, « Marx et Engels face à la question de l'esclavage » in MONTAUBAN Jean-Gabriel et MIGNOT Dominique-Aimé (dir.), *Esclavage et servitude aux Antilles : l'héritage antique et médiéval – XVIIe-XXe*, 2015

207ELLUL Jacques, *Le Système technicien*, Calmann-Lévy, 1977

« l'État [est le] point de départ de toutes les réflexions en ce domaine [de l'ordre juridique]. (...) L'ordre juridique est une espèce du genre plus général "ordre normatif", notion qui renvoie à tous les phénomènes constitués par des ensembles comportant des propositions énonçant des devoir-être adressées à des personnes humaines, autrement dit des propositions normatives. On y trouve, à côté du droit, la morale, la religion, les mœurs mais aussi les jeux qui comportent, par définition, des règles constitutives énonçant ce que les personnes doivent faire si elles désirent jouer à tel ou tel jeu. ».

C'est par contraste avec la normativité étatique qu'est identifié un ordre normatif parallèle : si le Droit appartient à l'État, la Morale, la Religion, les Mœurs ou les Jeux sont des ordres normatifs extra-étatiques. Pour le civiliste Jean Carbonnier, le « non-droit » est une situation naturelle dès lors que la société humaine serait, de fait, régie par un « pluralisme normatif »²⁰⁸ qui empêche l'accaparement de la société par la seule norme juridique. Après une enquête empirique en Colombie, la pénaliste Diana Villegas conclut à l'existence d'un « ordre mafieux » autonome, concurrent normatif (et même « juridique ») direct de l'ordre étatique²⁰⁹. L'affranchissement de ces normes et ordres juridiques par rapport à l'institution communautaire officielle, à l'État, leur réalité malgré leur inexistence *en tant qu'étatiques* ouvre l'analyse à leur existence *en tant que tels*. L'autonomie juridico-étatique sert de modèle comparatif pour détecter d'autres modèles normatifs autonomes.

Classiquement, la recherche juridique d'une autonomie normative s'appuie donc sur la démonstration d'une indépendance normative par rapport à l'État, terrain sur lequel se placeront les théoriciens « endogénistes » du droit d'internet. Régulièrement cité par les juristes bien qu'il n'en soit pas un lui-même, John Perry Barlow fut l'un des premiers à affirmer l'autarcie normative du réseau numérique par rapport à l'État dans sa « *Déclaration d'indépendance du cyberspace* » diffusée sur le Web en février 1996 :

« Gouvernements du monde industriel, (...) vous n'avez pas de souveraineté où nous nous rassemblons. Nous n'avons pas de gouvernement élu, et il est improbable que nous en ayons un jour. (...) Vous n'avez aucun droit moral de dicter chez nous votre loi et vous ne possédez aucun moyen de nous contraindre que nous ayons à redouter. (...) Le Cyberspace ne se situe pas dans vos frontières. (...) C'est un produit naturel, et il croît par notre action collective. (...) Où il y a des conflits réels, où des dommages sont injustement causés, nous les identifierons et les traiterons par nos propres moyens. (...) Vos concepts légaux de propriété, d'expression, d'identité, de mouvement (...) ne s'appliquent pas à nous. Ils sont basés sur la matière, il n'y a pas ici de matière. »

Ancien parolier des *Grateful Dead*, libertarien, J. P. Barlow s'était illustré en 1990 pour avoir co-initié l'*Electronic Frontier Foundation* (EFF) avec Mitch Kapor et John Gilmore, une association de défense des droits et libertés au contact des technologies. Créateurs du

208CARBONNIER Jean, *Sociologie juridique*, Quadrige Manuels, 2016 [1^{ère} éd. en 1972]

209VILLEGAS SANTIAGO Diana Milena, *L'ordre juridique mafieux : étude à partir du cas de l'organisation criminelle colombienne des années 1980 et 1990*, Dalloz, 2018 [1^{ère} publ. en 2016]

Cyberspace Law Institute en 1996, David R. Johnson (ancien directeur de l'EFF en 1993 puis ancien président en 2005) et David G. Post reprennent l'année suivante²¹⁰ l'argument érigé sur l'aspect immatériel, « virtuel » du réseau numérique. Dans un premier temps, les deux universitaires spécialisés en droit des nouvelles technologies arguent l'incapacité structurelle de l'État à régir internet : en tant que système de régulation, le Droit est tout entier « *fondé sur des frontières entre espaces physiques* » car émanant d'États dont le territoire, la population et les gouvernements²¹¹ les séparent physiquement et institutionnellement les uns des autres. Or, internet met à disposition des données accessibles ou produites depuis n'importe quel lieu géographique, en sorte que serait remise en cause « *la capacité de l'emplacement physique à indiquer la règle applicable* ». Dans un deuxième temps, les auteurs attribuent cette impuissance étatique à un « espace » normativement autonome – le « cyberspace », notion imaginée par l'auteur de sciences-fictions William Gibson en 1984 pour dépeindre une animation virtuelle (actions effectuées selon les règles du réseau par ses membres) abstraite de la structure matérielle (électrodes de connexion au réseau régies selon leur lieu d'existence urbaine)²¹². Existerait un « monde du bit » dans lequel les comportements logiciels ne répondent pas aux règles matérielles du « monde de l'atome ». Dès lors, « *parce que le Net est conçu pour fonctionner sur la base d'emplacements « logiques », et non géographiques, toute tentative visant à briser l'indépendance des communications à l'égard des emplacements physiques serait aussi futile qu'un effort visant à souder ensemble un atome et un bit* »²¹³.

L'existence d'une autonomie immatérielle, logicielle fut une première voie pour la démonstration juridique d'une autarcie normative en ligne. Une deuxième voie empruntée par James Boyle (bénéficiaire du Prix Pionnier de l'EFF en 2010 pour le récompenser de ses apports dans l'émancipation numérique de l'être humain) consiste à démontrer l'impossibilité technique de pénétrer la normativité du réseau²¹⁴. D'abord, soutient-il, l'architecture maillée d'internet rend impossible le contrôle d'un nœud central, provoquant ainsi une « *Carotte libertaire* » (« *libertarian Gotcha!* ») qui piègerait le censeur dans une impasse : « *le Réseau est à l'image d'un robinet qui n'a que deux réglages : soit il est en marche, soit il est à l'arrêt. Une fois en marche, tout vous est accessible* ». Ensuite, *a contrario* des autres biens, la consommation d'une information par une personne ne diminue pas la consommation que peut en faire une autre personne et son usage peut alors être simultanée sans déperdition de l'information, rendant non appropriable un cyberspace intégralement composé d'informations. Enfin, toute tentative de fractionner nationalement internet pour y superposer les règles locales des États serait vaine compte tenu de l'accessibilité mondiale du réseau internet – il suffit d'un seul État admettant la

210JOHNSON David R. et POST David G., « Law and Borders – the Rise of Law in Cyberspace », *Stanford Law Review*, vol. 48, 1996, p. 1367s.

211Soit les trois éléments classiquement définitoires de l'Etat en droit international

212GIBSON William, *Neuromancer*, Ace Books, 1984

213Cette théorie a suscité de nombreuses oppositions (outre celles attendues du côté hardwariste) pour l'indépendance radicale et totale qu'elle alloue à un cyberspace virtuel à l'égard de ses attaches matérielles. Par ex., en droit, v. COHEN Julie, « Cyberspace as/and Space », *Columbia Law Review*, vol. 107, 2007, p. 217 : « *la variante utopique d'un exceptionnalisme du cyberspace a pu être qualifiée de "naïve" (quant à la nature humaine et les réalités du pouvoir) et "essentialiste" (quant à la nature de l'Internet)* ». En théorie des réseaux sociaux, v. JURGENSON Nathan, « When Atoms Meet Bits : Social Media, the Mobile Web and Augmented Revolution », *Future Internet* 4, n° 1, 2012, p. 83-91

214BOYLE James, « Foucault in Cyberspace » [en ligne sur le site web de la revue], *Yale Journal of Law and Technology*, vol. 2, 2000

légalité d'une activité en ligne condamnée par tout autre État pour que cette activité soit accessible à tout endroit du monde, produise des effets là où elle est légalement interdite. Triplement bunkerisée contre une potentielle régulation étatique, la structure technique d'internet favorise l'épanouissement d'une normativité autarcique inarrêtable par l'État.

Une troisième voie démonstrative est proposée par la thèse de Yochai Benkler : l'autonomie du réseau peut encore se manifester par l'existence d'une économie qu'il porterait en lui-même²¹⁵. Jusqu'à la naissance d'un réseau numérique ouvert et maillé, seules la presse, les chaînes TV et la radio participaient à l'« *économie de l'information* » ; avec internet, l'économie de l'information s'enrichirait de toutes les « *actions individuelles décentralisées* » des utilisateurs du réseau. Cette extension et cette décentralisation de l'économie de l'information emporteraient trois effets : (i) dans un environnement purement immatériel, tombe la barrière matérielle posée par le modèle propriétaire ; (ii) l'économie de l'information n'est plus seulement constituée de productions marchandes (TV, presse...) mais aussi de productions non-marchandes provenant d'actions communes d'utilisateurs éparpillés ; (iii) en conséquence de quoi naissent de nouveaux efforts de coopération que Y. Benkler baptise « *peer-production* » (« production par les pairs ») et qui consiste en une production commune non-propriétaire et décentralisée « *de l'information, du savoir et de la culture* ». Succédant à l'« *économie de l'information industrielle* », cette « *économie de l'information en réseau* » serait due au fait que « *la technologie crée des espaces de faisabilité pour la pratique sociale* »²¹⁶. En attesteraient les activités de partage culturel en ligne (films, musiques, jeux-vidéos...), les projets collaboratifs (wikis, financements participatifs avec le *crowdfunding*, les cagnottes...) ou encore la « communauté du libre » (qui, par opposition aux logiciels propriétaires, met à disposition les « codes sources » de ses logiciels, i.e. leur composition sous forme de langage informatique, afin d'en permettre la libre et constante amélioration par les autres développeurs). Inexistant par le passé, ce nouveau paradigme économique fait des membres du réseau (développeurs, utilisateurs...) les autorégulateurs de la valeur économique des biens-informations. Aucune économie ne pouvant surgir sans comportement normatif à sa base, l'essor d'une économie depuis le réseau reflète la normativité de ce dernier.

Dans le discours juridique endogène, le « Cyberspace » – ou plus sobrement « Réseau » chez Y. Benkler – renvoie donc à une unité normative (par son architecture, son accessibilité universelle, son économie, les comportements logiciels qu'il abrite...) **identifiée à partir de son autarcie vis-à-vis de l'ordre juridique et régie par la technologie en réseau.** Restait à constater ces « règles internes au cyberspace » pour confirmer l'hypothèse endogène.

B) Le jeu normatif par le langage informatique : Code is Law

À ce jour, l'hypothèse la plus exploitée de ces règles internes au cyberspace les tirent du « code source ». On connaît déjà le code binaire, exclusivement comblé de 0 et de 1 et tout aussi exclusivement compris des seules machines numériques. Une catégorie de personnes – les développeurs de logiciels – s'est toutefois efforcée de rendre ce code binaire utilisable conformément à l'entendement humain. L'enjeu : si l'être humain peut faire correspondre une formule qu'il comprend à une suite de 0 et de 1, la machine connaîtra l'action à exécuter *chaque fois qu'elle lira cette formule*. Le développeur n'a qu'à sélectionner les formules qui

215BENKLER Yochai, *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, 2006 [en ligne sur benkler.org]

216Ibid., p. 31

l'intéressent pour créer un ensemble d'instructions, *i.e.* un logiciel. Ces formules et leurs logiques de structuration diffèrent selon leur langage d'appartenance : les formules d'un langage « bas-niveau » (C, C++...) s'adressent aux composantes matérielles de la machine comme la mémoire interne, tandis que les formules d'un langage « haut-niveau » (Python, JavaScript...) abstraient leurs instructions de ces composantes matérielles²¹⁷. De ce fait, les possibilités technologiques varient d'un langage à un autre. Écrites en *code source*, ces formules extraites de tel ou tel langage sont ensuite traduites en *code binaire* par un autre logiciel dit « compilateur », programmé avec les concordances < X formule = X signal numérique > afin que la machine comprenne les instructions exprimées par les formules. Coexistent ainsi deux codes informatiques : le code binaire déchiffrable par la seule machine ; et le code source lisible par le seul être humain. **Le code source d'un logiciel désigne ainsi la composition de ce dernier sous forme de langage informatique.** La présence sur le réseau de codes sources logiciels maîtrisés et manipulés par un petit nombre a fait s'interroger sur trois points fondamentaux les scientifiques qui étudient les rapports de force en ligne depuis les jeux normatifs « internes » au réseau : l'utilisateur d'un logiciel dépend-il du code source écrit par le développeur *via* un langage informatique, dans quelle mesure et pour quelles conséquences ?

La problématique n'est pas totalement nouvelle, et s'était déjà posée dans le milieu littéraire de la fin des années 1960. Entre 1968-69, Roland Barthes et Michel Foucault lançaient le mouvement littéraire sur « *La Mort de l'Auteur* »²¹⁸ philosophiquement imprégné des théories structuralistes. Schématiquement, on peut retenir le structuralisme comme une conception endogène de la littérature, portant non plus sur l'objet technique mais sur le langage. Pour les philosophes structuralistes en effet, le langage est assimilable à une structure, une ossature, à la représentation mathématique d'un système. Prenons la figure géométrique du triangle équilatéral²¹⁹ : son aire, ses angles, ses côtés, son périmètre... toutes ses caractéristiques peuvent être calculées à l'aide de règles mathématiques connues (loi des cosinus découverte par Al-Kachi, axiomes dégagés par Euclid, théorème de Pythagore...). La structure « triangle » obéit à la cohérence des règles du système « mathématique », lequel système comporte dès lors des règles internes dont l'être humain ne peut ni contester ni modifier la réalité, mais qu'il peut découvrir et utiliser. Par analogie, les structuralistes voient le « langage » comme la structure de modélisation d'un système « sémantique » dont la cohérence des règles internes recèlerait une réalité à investiguer. Désireux de prouver l'existence de cette réalité derrière la structure, R. Barthes tente d'abord de s'exprimer sans passer par les contraintes structurelles du style ou de la langue²²⁰ : tout comme l'étendue des mathématiques ne saurait être couverte par la structure contraignante du triangle, l'étendue de la sémantique ne saurait être exploitée par la structure contraignante du langage.

217On examinera plus loin le fonctionnement des langages informatiques et leur action auprès de la machine numérique

218BARTHES Roland, « The Death of the Author », *Aspen Magazine*, n° 5/6, 1967 ; FOUCAULT Michel, « Qu'est-ce qu'un auteur », *Bulletin de la Société française de philosophie*, n°3/63^e année, 1969 (conf. de 1968)

219La géométrie sert à simplifier la démonstration, les structuralistes s'inspirant davantage de l'algèbre moderne : RABOUIN David, « Chapitre I. Structuralisme et comparatisme en sciences humaines et en mathématiques : un malentendu ? », in MANIGLIER Patrice (dir.), *Le Moment philosophique des années 1960 en France*, PUF, 2011, p. 37-57. Aussi, plus complètement, DOSSE François, *Histoire du structuralisme*, La Découverte, 2012 (2 tomes)

220BARTHES Roland, *Le degré zéro de l'écriture*, Seuil, 1953

Par la « Mort de l'auteur », le lecteur retrouverait la liberté de s'épanouir dans le système sémantique, s'émanciperait des contraintes langagières ou littéraires structurées par l'auteur. En 1979, cette dépendance structurelle du lecteur au narrateur sera brillamment démontrée par Italo Calvino, dont la filiation structuraliste barthésienne est établie²²¹. En parcourant les pages de son (pluri-)roman *Si par une nuit d'hiver un voyageur*, le lecteur est subtilement piégé par sa propre dépendance aux structures littéraires. Au premier stade du récit, I. Calvino emploie des structures oulipiennes, inspirées du mouvement littéraire de l'OuLiPo (Ouvroir de littérature potentielle) qui joue de la cohérence des règles syntaxiques et littéraires pour énoncer des problèmes à résoudre selon lesdites règles²²². Au deuxième stade de la narration, il décrit, parfois à la deuxième personne du singulier, la quête par le héros nommé « Lecteur » d'un manuscrit-graal à travers dix *incipit* successifs dont, par définition, aucun n'a de fin. La relation introspective auteur-lecteur-narrateur éprouve le raisonnement du lecteur, le sens de l'histoire est difficile d'accès, et pourtant, en respectant rigoureusement les règles littéraires selon la méthode scientifico-oulipienne, I. Calvino conforme son récit au même système que celui dont provient toute œuvre écrite dans la même langue. Il prouve par là au lecteur que son accès à un même système peut être contrarié, manœuvré selon les structures choisies par l'auteur.

Les mêmes conséquences peuvent-elles être déduites du rapport utilisateur-développeur ? Soit, dans quelles limites la normativité pour le lecteur d'une rédaction en langage urbain est-elle comparable à la normativité pour l'utilisateur d'une rédaction en langage informatique ?

Dès 1984, la socio-psychologue Sherry Turkle constatait que l'utilisation du réseau numérique engendre des réflexes cognitifs spécifiques du côté de l'utilisateur²²³. Loin d'en faire un usage externe et distant, l'utilisateur *intégrerait* psychologiquement les mécanismes et la disposition du réseau, déclenchant ainsi une intimité Homme-Machine qui changerait la direction sociale²²⁴. Étayant trois types d'associations cognitives, S. Turkle livre en 1995²²⁵ les résultats de ses enquêtes de terrain qui concrétisent la fusion psychique Homme-Machine entrevue onze ans plus tôt. D'abord, la transformation par l'ordinateur de calculs électriques en interfaces graphiques permet d'utiliser cet ordinateur selon la compréhension humaine, laquelle compréhension associe à la machine les possibilités d'utilisation offertes par l'interface graphique et ses utilisations effectives. Ensuite, les progrès de l'intelligence artificielle atténueraient la dissociation spirituelle entre le vivant et le non-vivant par la réplique réifiée d'une faculté jusqu'ici reconnue au seul être humain – le raisonnement, quoique l'enfant distancierait davantage l'Homme de la Machine. Enfin, une troisième association cognitive Homme-Machine est visible auprès des communautés en ligne, dont les membres se confondent avec l'identité virtuelle qu'ils s'octroient. Cette hypothèse, qui unit une même personne à une fragmentation d'identités cloisonnées les unes des autres selon ses communautés

221MONLUÇON Anne-Marie, « Entre théorie et fiction : quelques figures paradoxales de l'Auteur dans *Si par une nuit d'hiver un voyageur* d'Italo Calvino », *Recherches & Travaux*, n° 64, 2004, p. 141-156

222LANGLOIS Sindy, « Si par une nuit d'hiver un voyageur : quand la fiction dépasse la fiction », *Littérature et mathématiques*, n° 68, 2002, p. 23-32. Précisons pour éviter toute confusion que contrairement au structuralisme, l'Oulipo ne s'émancipe pas des contraintes structurelles mais en joue

223 TURKLE Sherry, *The Second Self : Computers and the Human Spirit*, HarperCollins, 1984

224TURKLE Sherry, « L'écran fragmenté », *Sociétés*, n° 79, 2003, p. 17 : « lorsque nous les utilisons, lorsque nous nous projetons dans leurs mondes, ces machines provoquent une réflexion sur notre vie et notre esprit. En ce sens, la vie à l'écran devient une philosophie quotidienne »

225TURKLE Sherry, *Life on the Screen: Identity in the Age of the Internet*, Simon & Schuster, 1995

d'appartenance, est confirmée par les enquêtes sociologiques récentes menées sur les réseaux sociaux à cette différence, depuis les années 1990, que le cloisonnement s'est dilué dans l'auto-exposition de soi et l'interconnexion des réseaux sociaux ²²⁶. L'établissement d'un lien psychologique entre l'Homme et la Machine fait remarquer à S. Turkle les pouvoirs cognitifs de l'auteur du logiciel à l'égard de l'utilisateur lors d'une enquête menée sur le jeu vidéo SimCity en 2001. Plusieurs de ses sujets d'études (des enfants) semblaient alors particulièrement réceptifs aux règles du jeu telles que programmées par langage informatique à l'instar de cette adolescente qui, invitée à lister les 10 règles principales du jeu SimCity d'après elle, y fait figurer celle selon laquelle « *l'augmentation des impôts entraîne toujours des émeutes* »²²⁷. S. Turkle y voit la naissance d'un « *lectorat dans la culture de la simulation* ».

Cette problématisation du rapport développeur/utilisateur suit un mouvement entamé depuis la fin des années 1990. Expérimentant le cas des jeux-vidéo en 1997, l'universitaire spécialisé dans les applications informatiques aux sciences humaines Manfred Kämmer relève que « *l'aventure du joueur de jeux informatiques est un voyage dans le cerveau du designer de software* »²²⁸. C'est toutefois en 1999 que cette emprise du développeur sur l'utilisateur est technologiquement – et non plus cognitivement ou socialement – imputée au code source par le juriste Lawrence Lessig. Le Professeur de droit constitutionnel compare le développeur à un « *faiseur de loi* »²²⁹ : en inscrivant les possibles et les interdits dans le code source du logiciel, les développeurs fabriqueraient les règles de conduite des utilisateurs. L'utilisateur d'un jeu vidéo peut-il (par simulation) tuer un autre utilisateur, avec quelle arme, pour quelles conséquences ? Le membre d'un réseau social peut-il « disliker » une publication Facebook, écrire des messages de plus de 240 caractères sur Twitter, vendre des photographies qui l'exposent nu (*nudes*) comme le propose OnlyFan ? Des règles les plus basiques comme la mort et la communication à celles les plus détaillées comme le commerce de son propre corps, toutes seraient décidées par le développeur. « *À moins que [le logiciel] ne soit libre et donc que son code soit aisément modifiable, l'utilisateur est à la merci du développeur qui a écrit le logiciel* »²³⁰. L. Lessig synthétise sa démonstration par la désormais célèbre formule « *Code is Law (in Cyberspace)* » (qu'on abrégera CodIL pour la suite). Le *Code* de cette locution ne renvoie donc pas au code binaire *matériellement* compris mais au code source dont la signification est *logicielle*. Le constitutionnaliste conçoit le Cyberspace indépendamment de ses attaches matérielles, comme un lieu de pouvoir logiciel régi par ses législateurs (les développeurs) et ses « *gouvernements* » (les « *marchands-souverains* »²³¹ pour le compte desquels travaillent les développeurs) avec ses citoyens (les internautes). La source de pouvoir ainsi localisée au niveau « virtuel » du réseau, L. Lessig dénie tout « essentialisme » (« is-ism »²³²) qui rendrait le Cyberspace incontrôlable par nature : la maîtrise sur le « Code » emporterait celle du Réseau.

226MERCKLÉ Pierre, *Sociologie des réseaux sociaux*, La Découverte, 2016, p. 71-94

227TURKLE Sherry, « Seeing Through Computers », *The American Prospect*, 2001 [en ligne sur le site prospect.org]

228Cité par PAPILLOU Christian, « L'interactivité. Le défi d'une sociologie des usages des TICs », in G. VIDAL (dir.), *La sociologie des usages*, préc., Lavoisier, 2012, p. 100

229LESSIG Lawrence, *Code: Version 2.0*, Basic Books, 2006 [1^{re} éd. 1999], p. 79 [en ligne]

230NITOT Tristan, *surveillance://*, Blogcollection, 2016, p. 72

²³¹ LESSIG Lawrence, *Code: Version 2.0*, préc., 2006, p. 287s.

²³² *Ibid.*, p. 31s.

L'explication CodIL est sans doute l'une des plus connues et relayées de la conception endogène aussi bien en droit qu'en sociologie ou en sciences de l'information et de la communication ²³³. Elle a évidemment suscité la contestation dans les premiers rangs hardwaristes, qui identifient strictement la source du pouvoir dans le matériel ²³⁴, et pragmatiques, qui rejettent la réalité d'un « cyberspace » par-delà la métaphore (v. *supra*). En identifiant le code source comme enjeu de pouvoir technique, il montre néanmoins que la compréhension humaine n'est pas le seul objet de dépendance dans la relation utilisateur-développeur : les capacités d'action, les *conduites* mêmes de l'utilisateur sont cadrées et réglementées par les choix du développeur.

Ceci admis, l'analogie entre la relation développeur-utilisateur et la relation auteur-lecteur bute sur une différence de taille. Les « structures » fournies par les développeurs (*i.e.* le code source) ne manœuvrent pas seulement l'esprit de l'utilisateur, mais ses capacités concrètes d'utilisation d'un objet ; et le « système » que recèle ces structures n'est dès lors pas sémantique ou linguistique mais actionnel. Si, comme le lecteur du roman, l'accès de l'utilisateur au système dépend effectivement des structures fixées par l'auteur, le pouvoir du développeur est d'une toute autre nature que celui de l'auteur littéraire puisqu'il se situe dans le champ opérationnel et non seulement spirituel ²³⁵. En situant le pouvoir du développeur dans la régulation des conduites, l'explication CodIL fait regarder ledit pouvoir comme un fait technique, vérifiable par la simple création ou utilisation d'un logiciel, démontrable dès le principe de fonctionnement d'un logiciel (créer telles fonctionnalités selon telles modalités sans quoi l'objet n'est pas utilisable). Sans nécessairement adhérer au mouvement CodIL le plus rigide (existence d'un cyberspace, domestication du réseau par un code minimalement contraint par le matériel...), de

233Par ex. en droit : RODA Jean-Christophe, commentaire sur « Taina Pihlajarinne, Juha Vesala et Olli Honkkila (éd.), *Online Distribution of Content in the EU* », *Revue trimestrielle de droit européen*, n° 1, 2020 (remarquant que « *le fameux Code is Law (...) devient presque une rengaine dès que le secteur du numérique est abordé* ») ; GODEFROY Lémy D., « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz*, n° 8, 2016, p. 438-444 ; le CodIL est surtout abordé par les juristes sous l'angle des plateformes, des objets connectés ou de la *blockchain* et des *smart contracts* qui l'accompagnent (v. notam. les divers travaux de Mustapha Mekki, de Myriam Quémener et de J.-C. Roda). En sociologie : FLICHY Patrice, *L'imaginaire d'Internet*, La Découverte, 2001, notam. p. 200s. ; BARDINI Thierry et PROULX Serge, « La culture du hack en ligne, une rupture avec les normes de la modernité », *Les Cahiers du numérique*, vol. 3, 2002, p. 35-54 ; BOULLIER Dominique, *Sociologie du numérique*, Armand Colin, 2019, notam. p. 223-285. En sciences de l'information et de la communication : PALOQUE-BERGÈS Camille, *Poétique des codes sur le réseau informatique*, Archives Contemporaines, 2009 ; BADOUARD Romain, MABI Clément, MONNOYER-SMITH Laurence, « Le débat et ses arènes », *Questions de communication*, n° 30, 2016 [en ligne] (rappelant que « *suivant la célèbre phrase de Lawrence Lessig selon laquelle, en ligne, "le code fait loi", un courant de recherche à la croisée des sciences de l'information et de la communication et des science and technology studies s'est, depuis le début des années 2000, intéressé à la manière dont les ressources techniques du numérique cadrent et orientent les pratiques délibératives et participatives en ligne* », citant les travaux de Nicolas Benvenuto, Lance Bennett, Scott Wright et John Street, Stephen Coleman etc.). Les philosophes ont aussi grandement contribué à la diffusion de la démonstration CodIL (au premier rang, en France, MATHIAS Paul, *Des libertés numériques*, PUF, 2008).

234WU Tim, « When Code Isn't Law », *Virginia Law Review*, vol. 89, 2003, p. 679-751

235On ne conteste pas que la littérature puisse influencer des actions sociales, voire conditionner le raisonnement selon les actions ou les logiques décrites par le romancier, de la même manière que l'utilisation du réseau internet peut influencer des actions sociales ; mais l'auteur littéraire n'exerce pas de pouvoir sur les facultés d'usage du lecteur.

nombreux chercheurs ont reconnu ce pouvoir du développeur comme un fait technique. Par reconnaissance et approfondissement de ce « fait technique », a ainsi pu s'ouvrir une combinaison des approches endogènes et exogènes pour cerner les rapports de force en ligne de façon panoramique.

Section 2. Normativités croisées au sein du cyberspace

Issu d'une articulation des leçons exogènes et endogènes, le constat scientifique d'une pluralité normative (Paragraphe 1) est adopté pour la régulation juridique des acteurs d'internet (Paragraphe 2).

Paragraphe 1 - Un éparpillement de foyers normatifs scientifiquement articulés

Par combinaisons des enseignements exogènes et endogènes, ont pu être désignées plusieurs sources de normativité communicationnelle (A), architecturale, pratique ou économique sur internet (B).

A) Une normativité communicationnelle en ligne

Les apports de la conception endogène d'internet ont rencontré principalement des problématiques venues de l'approche communicationnelle-informationnelle, qui corréle la donnée à une information-expression humainement comprise plutôt qu'à une information-bien exploitée économiquement par les êtres humains [*supra*]. Si le réseau internet est régi *en son sein* (du moins pour partie), quelles sont les conséquences de ces règles sur les communications qui le traversent ? Comment la compréhension humaine, externe au réseau, réagit-elle mise en contact avec les règles « au-dedans » du cyberspace ?

Philosophe de la technique, Bernard Stiegler analyse l'esprit humain comme un ensemble de « *flux de conscience* » qui obéiraient à des lois temporelles consécutives ²³⁶ . Ces flux démarreraient par le premier temps de l'*attention*, c'est-à-dire l'activation de la conscience, la mise en branle des capacités perceptives ou cognitives humaines. Ils atteindraient ensuite le temps de la *réention*, qui correspond au déclenchement des capacités mnésiques humaines, la « mémoire ». Ces flux termineraient leur trajet au troisième temps de la *protention*, où sont mobilisées les capacités rationnelles de l'Homme qui font naître le questionnement, l'attente, le désir etc. B. Stiegler s'attarde notablement sur le temps de la réention qu'il subdivise en trois sous-temps : les réentions primaires relèvent d'une mémoire à court terme qui capterait les informations dernièrement survenues (perception) ; les réentions secondaires relèvent d'une mémoire à moyen terme qui capterait les souvenirs issus des réentions primaires (imagination) ; les réentions tertiaires relèvent d'une mémoire à long terme qui capterait les connaissances accumulées au fil de l'évolution humaine (génération). Chronologiquement, les éléments perçus deviennent imaginés avant de s'insérer dans l'avancement générationnel. Mais en sens inverse aussi, chacun de ces trois niveaux de réention surdéterminait le précédent à la manière d'une cascade inversée : la mémoire à long terme surdéterminerait celle à moyen terme, qui surdéterminait celle à court terme. Nos perceptions immédiates seraient inclinées par nos antécédents générationnels.

236STIEGLER Bernard, *La technique et le temps. Tome 3. Le temps du cinéma et la question du mal-être*, Galilée, 2001, p. 21s.

La personne humaine d'aujourd'hui se déduirait donc de toutes les extériorisations qui lui parviennent ou qui lui sont parvenues²³⁷, de toutes les expressions auxquelles sa conscience accède et qu'elle *retient*. Pour B. Stiegler, il ne fait pas de doute que, au nombre des extériorisations devenant des rétentions tertiaires qui imprègnent la mémoire générationnelle, figurent les expressions communiquées par la machine numérique comme, autrefois, celles communiquées par voie papier²³⁸. À la différence du papier toutefois, la machine numérique est « automatique » : elle a certes besoin du sujet humain pour la fabriquer, mais n'en a guère besoin pour travailler ; « *l'objet travaille de lui-même* » sans intervention humaine nécessaire²³⁹. L'automatisation serait aggravée par l'algorithmie logicielle. En soi, un algorithme n'est rien d'autre qu'une succession d'étapes à respecter méthodiquement pour résoudre un problème (enchaînement de calculs mathématiques pour attribuer une valeur mathématique au résultat recherché, manipulations à répéter pour homogénéiser les faces d'un Rubik's cube, gestes-barrières à suivre pour contenir une épidémie, recette de cuisine pour réussir un repas...). Seulement, une fois l'algorithme retranscrit dans le code source d'un logiciel, ces étapes sont automatiquement exécutées par la machine numérique. Quand un utilisateur se sert d'un tel logiciel, il *retient* donc les expressions, les *externalisations* formulées par cet algorithme et automatisées par la machine.

Sur cette théorisation, le philosophe envisage deux *scenarii* contraires²⁴⁰ : (i) soit l'utilisateur absorbe passivement ces informations algorithmiques sans interroger, sans raisonner, sans « re-intérioriser » les externalisations reçues, auquel cas ses rétentions seront le fruit d'expressions automatisées et son unicité, son individuation se fondra dans l'objectivité statistique ; (ii) soit il comprend le fonctionnement de l'écriture numérique (du code source), ses implications et ses biais, auquel cas les rétentions de l'usager capteront de nouvelles réflexions et connaissances *personnelles* en plus des informations reçues, enrichissant et améliorant ainsi l'individuation de la *personne* humaine. B. Stiegler s'inquiète toutefois du succès de la première hypothèse qui produirait une « *externalisation sans retour, sans intériorisation en retour* », instituerait une domination unilatérale (de ceux qui maîtrisent le code source sur les analphabètes de l'écriture numérique) caractéristique d'une « *prolétarianisation* »²⁴¹. Les décisions automatisées prises par l'auteur de l'algorithme, externalisées par le logiciel, domineraient le temps des rétentions et, par ricochet, les deux autres temps parcourus par les flux de conscience humaine ; les extériorisations automatiques retenues influeraient sur le temps de la protention (nos attentes, nos désirs...) qui, à son tour, rétroagirait sur le premier temps de l'attention (ce à quoi nous sommes réceptifs). Dans cette « *société de l'hypercontrôle (...)* fondée

237STIEGLER Bernard, conférence « L'extériorisation de la mémoire et ses conséquences », 2014 [en ligne sur franceculture.fr]

238STIEGLER Bernard, *La société automatique. 1. L'avenir du travail*, Fayard, 2015, p. 57 : « *au même titre que les traces écrites dans lesquelles Socrate voit déjà le risque de prolétarianisation que comporte toute extériorisation du savoir – le paradoxe apparent étant qu'un savoir ne peut se constituer que par son extériorisation –, les traces numériques, analogiques et mécaniques sont des rétentions tertiaires* »

239Dialogue entre Michel Serres et Bernard Stiegler animé par Martin Legros pour Philosophie Magazine, publié le 4 sept. 2012 : <https://www.my-mooc.com/en/video/dialogue-michel-serres-et-bernard-stiegler-complet/>

240Comme tout objet, la technologie aurait les propriétés d'un *pharmakon*, à la fois poison et remède de l'hominisation : STIEGLER Bernard, « Questions de pharmacologie générale. Il n'y a pas de simple *pharmakon* », *Psychotropes*, 2007, vol. 13, p. 27-54

241STIEGLER Bernard, *La société automatique.*, préc., Fayard, 2015, p. 57

sur l'exploitation industrielle, systémique et systématique des rétentions numériques par où tous les comportements sont générateurs de traces et toutes les traces sont objets de calcul », il y aurait « *captation destructrice de l'attention et du désir* »²⁴². La conscience humaine serait tout entière guidée par les externalisations des nouveaux dominants numériques dont l'utilisateur inaverti serait l'automate.

On ne s'étonnera pas, alors, que B. Stiegler s'accorde avec la « *gouvernementalité algorithmique* » dénotée en 2013 par la philosophe du Droit Antoinette Rouvroy et le philosophe politique Thomas Berns. Les concepteurs d'algorithmes autant que leurs entreprises bénéficiaires (réseaux sociaux, moteurs de recherche, services de *streaming* ²⁴³ ...) exerceraient cette gouvernementalité suivant trois étapes. Premièrement, seraient extraites les « *multiples facettes du réel* » à l'aide « *des informations abandonnées [par les utilisateurs] plus que cédées, des traces laissées et non des traces transmises* », collectées pour attribuer à ces facettes, « *dans leur totalité* », un double statistique qui ne répond d'aucune signification collective (valeurs morales, lois...) mais relève d'un strict « *dédoublement du réel* » ²⁴⁴ . Traduisant un « *comportementalisme numérique généralisé* », ce double fidèle à la réalité est, deuxièmement, transformé par des corrélations algorithmiques en un « *savoir* » méconnu des utilisateurs, en un double augmenté selon les critères de l'algorithme. Troisièmement, de ces « *savoirs* », les exploitants commerciaux qui y ont accès peuvent en tirer des probabilités statistiques « *à des fins d'anticipation des comportements individuels* » et intégrer dans le logiciel des règles algorithmiques destinées à orienter ces comportements. C'est là qu'il y a « *application de la norme sur des comportements* » ²⁴⁵ : l'obtention d'un crédit (par un algorithme bancaire), la tarification d'un contrat d'assurance, l'organisation d'un rendez-vous médical (Doctolib), l'approvisionnement alimentaire (UberEats, Deliveroo, Carrefour, Monoprix...), les découvertes musicales (YouTube, Deezer, Spotify, SoundCloud...) etc. se feraient tributaires de normes comportementales fixées par algorithme. La conclusion de ces deux philosophes est alors proche de celle de L. Lessig, qui percevait l'incarnation d'un « *gouvernement* » par des « *souverains-marchands* » au moyen du code source rédigé par le développeur-législateur.

En 2016, la *data scientist* (analyste de données sur la base de modèles mathématisés) Cathy O'Neil dénonce l'éventualité pour tout algorithme de muer en une « *Weapon of Math Destruction* » cumulativement caractérisée par²⁴⁶ : (i) l'opacité de son fonctionnement voire de ses décisions ; (ii) l'impossibilité de remettre en cause ces décisions ; (iii) l'irresponsabilité des concepteurs/exploitants, i.e. leur inconscience des risques dommageables ou leur conscience de ces risques oblitérée par des ambitions économiques ; et (iv) la mauvaise conception à cause de laquelle l'algorithme traite des informations non-pertinentes par rapport à son objectif (critères biaisés, déductions algorithmiques faussées voire offensantes...). Parmi la foule d'exemples recensée par la mathématicienne, on reprendra celui du LSI-R (*Level of Service Inventory - Revisited*), un questionnaire fédéral rempli par les détenus et duquel les services de police américains en infèrent le potentiel récidiviste de chaque répondant. Nonobstant la neutralité et la pertinence

²⁴² *Ibid.*, p. 56-57

²⁴³ Le *streaming* consiste à fournir des services de vidéo en continu (YouTube, Twitch, Netflix, Disney+...)

²⁴⁴ ROUVROY Antoinette et BERNIS Thomas, « Gouvernamentalité algorithmique et perspectives d'émancipation », *Réseaux*, n° 177, p. 169

²⁴⁵ *Ibid.*, p. 171

²⁴⁶ O'NEIL Cathy, *Weapons of Math Destruction*, Crown Books, 2016, p. 1-18

des questions posées (par ex., « quelle est la première fois que vous été impliqué avec la police ? »), le LSI-R reproduit en fait le modèle raciste socialement ambiant (le potentiel récidiviste du répondant sera augmenté par son âge et son origine ethnique dès lors que les contrôles de police impliquent largement des hommes noirs et latino-américains de 14 à 24 ans, pourtant très minoritaires dans la population et reconnus innocents 9 fois sur 10 à l'issue d'un contrôle²⁴⁷). Le LSI-R se changerait ainsi en une *Weapon of Math Destruction* (i) opaque (comment exactement est évalué le potentiel récidiviste, selon quels coefficients, quels ratios, pour quelles leçons tirées dans une enquête etc. ?), (ii) incontestable (les résultats du LSI-R ne sont pas susceptibles d'appel), (iii) génératrice de dommages conséquents (ici les suites de l'enquête dirigée contre une personne) et (iv) « mal » conçue (en automatisant des biais racistes dans le rendu des décisions policières voire judiciaires si les magistrats s'inspirent de ces résultats pour la fixation de la peine, telle la Cour Suprême du Wisconsin avec l'algorithme COMPAS). Aux conséquences parfois très déterminantes (les fluctuations des cours de la bourse, l'admission d'un étudiant à l'université...), ces *Weapons of Math Destruction* varieraient dans leur gravité selon un triple²⁴⁸ : degré d'opacité ; degré dommageable (mesure dans laquelle l'algorithme endommage des vies humaines) ; degré d'application (échelle géographique, populationnelle, infrastructurelle... à laquelle s'appliquent les résultats de l'algorithme).

La démonstration a pour intérêt premier de refléter combien des résultats algorithmiques peuvent être *décisifs*, et le sont en fait. Les *décisions* issues de ces résultats peuvent encore servir des fonctions très diverses, à plus forte raison lorsque l'algorithme est intégré dans un logiciel, telles que : l'analyse (le logiciel d'appartenance de l'algorithme corrèle des informations pour en tirer des conclusions, comme décrit par A. Rouvroy et T. Berns) ; la prédiction (le logiciel suggère des comportements comme les « articles pertinents pour vous » des places de marché en ligne, les recommandations musicales ou cinématographiques etc.) ; la coercition (le logiciel applique une sanction à une ou plusieurs informations comme une suppression, une invisibilisation, un avertissement, une suspension en guise de sanction temporaire etc.) ; le tri (le logiciel organise l'expérience de l'utilisateur en sélectionnant les informations lui parvenant comme les extraits valorisés dans les *stories* des réseaux sociaux, les pages d'accueil personnalisées des sites web, les publicités adaptées aux intérêts de l'utilisateur etc.) ; la surveillance (le logiciel repère les informations à partir d'une suite de caractères dont on cherche le bannissement, des adresses IP impliquées dans une suspicion, l'activation par l'utilisateur de certaines fonctionnalités pour comprendre son comportement²⁴⁹ etc.) ; la validation (le logiciel vérifie l'exactitude de l'information par rapport à une réalité jugée valable comme les CAPTCHA qui s'assurent de l'identité humaine de l'utilisateur, les processus de confirmation de commande, la vérification de la majorité ou de la capacité de l'utilisateur par signature électronique etc.)... Chacune de ces fonctions suit les règles de l'algorithme, les étapes fixées pour résoudre un problème désigné ; ces fonctions sont par ailleurs assemblables – un « algorithme de modération » incorpore souvent des fonctions de coercition et de surveillance, voire d'analyse.

Les règles de l'algorithme sont ainsi à même d'orienter les comportements par le truchement du logiciel. Leur action normative complète ainsi celle des fonctionnalités, du *design*. Ex-déontologue *design* embauché par Google, Tristan Harris témoigne y avoir « étudié

²⁴⁷ Une étude réalisée par l'ACLU (*American Civil Liberties Union*) de New York en 2013 révélait que les hommes noirs et latino-américains de 14 à 24 ans ne représentaient que 4,7% de la population de la ville mais 40,6% des contrôles de police tandis que plus de 90% des personnes arrêtées étaient innocentes : *ibid.*, p. 28s.

²⁴⁸ *Ibid.*, p. 34s.

²⁴⁹ Par ex., en comparant l'activité des célibataires avec celle des couples, Facebook s'est affirmée capable en 2014 de déceler les couples non officialisés ou potentiellement en devenir à partir de leurs usages des fonctionnalités fournies par la plateforme (visites de profils, interactions...) : DIUK Carlos (*data scientist*), « The Formation of Love », 11 fév. 2014, étude pour le compte de Facebook [en accès libre sur sa plateforme]

comment orienter les pensées des gens de façon éthique » dans le but de « maximiser le temps d'attention accordé »²⁵⁰. En 2016 déjà²⁵¹, il partageait certains mécanismes d'orientation comportementale. Par exemple, la « récompense par intermittence variable » consiste à renforcer l'additivité de l'utilisateur à une technologie par l'envoi de notifications épisodiques destinées à faire naître la peur d'en rater une substantielle. Ou encore, jouant sur la « vulnérabilité à l'approbation sociale », les réseaux sociaux rendent les gestes interactifs les plus simple, rapide et intuitif possibles pour créer un geste retour de la part du destinataire par « réciprocité sociale ». Une étude dévoilée six mois plus tard par des chercheurs spécialisés en sciences de l'information corrobore l'existence d'une telle vulnérabilité auprès de 718 volontaires sondés : la fonctionnalité qui avertit l'auteur d'un message de son ouverture par le destinataire (« message vu/lu », notification d'ouverture du message...) fait germer chez ce destinataire une anxiété le pressant de répondre ou d'omettre délibérément le message, suscitant la colère chez 30% des expéditeurs voire 42% si le message est ouvert sans réponse²⁵².

Les diverses méthodes évoquées (fonctions algorithmiques, techniques d'orientation cognitive...) évolueront avec les prochaines découvertes, mais une conclusion scientifique stable s'impose à ce stade : **la modification du code source infléchit effectivement les issues décisionnelles et les faits sociaux, les comportements et utilisations, les états émotionnels et psychologiques.**

Dans ce rapport de force entre l'auteur et l'utilisateur du code source, l'utilisateur serait dominé plus que dominant sur le plan communicationnel. Il ne serait cependant pas dépourvu de tout pouvoir sur ce même plan d'après certaines analyses. Employant souvent la comparaison avec le *Global Village* de Marshall McLuhan, certains auteurs en sciences sociales maintiennent une lecture habermassienne d'internet²⁵³, y voient l'exaltation du pouvoir expressif des utilisateurs²⁵⁴, le moyen de contourner la censure ou d'étendre la portée de leurs

250V. la Conférence TED de HARRIS Tristan, « How a Handful of Tech Companies Control Billions of Minds every day ? », sur *Ted.com*, avr. 2017

251HARRIS Tristan, « How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist », sur *Medium.com* (hébergeur blog), mai 2016

252HOYLE Roberto, DAS Srijita, KAPADIA Apu, LEE Adam J. et VANIEA Kami, « Was my message read ? : Privacy and Signaling on Facebook Messenger » [en ligne], in *CHI'17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, p. 3838-3842. On ignore si ces résultats sont toujours d'actualité aujourd'hui sous l'effet de l'habitation sociale.

253Par ex., en droit, ROUSSEAU Dominique (« Introduction », in ARLETTAZ Jordane et LE BOT Olivier (dir.), *La démocratie en un clic*, L'Harmattan, 2010 ; « Le numérique, nouvel objet du droit constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel* (NCC), n° 57, 2017). En sciences de l'information et de la communication : MAROCCIA Michel (« La normalisation des comportements communicatifs sur internet : étude sociopragmatique de la nétiquette » in GUÉGEN Nicolas et TOBLIN Laurence (dir.), *Communication, société et internet*, L'Harmattan, 1998, p. 15-22 ; v. la plupart de ses autres travaux), KREBS Viola (*Le Cybervolontariat : sociopragmatique d'une activité citoyenne au XXIe siècle*, 2014 [en ligne sur theses.fr]). En sociologie : TUFEKÇI Zeynep, *Twitter and Tear Gas : The Power and Fragility of Networked Protest*, préc., YUP, 2017 ; v. aussi les synthèses théoriciennes de MATTELART Armand et MATTELART Michèle, *Histoire des théories de la communication*, La Découverte, 2018, notam. l'introduction et le VII. (p. 92-109)

254Par ex. en droit : SUNSTEIN Cass, *Republic.com*, Princeton University Press, 2001

expressions²⁵⁵, le vecteur de communautés en ligne dont les nouvelles propriétés spatio-temporelles réorganisent les jeux de pouvoir en société²⁵⁶. Dans ce cas, lorsqu'elles sont identifiées comme telles, les « normes » proviennent des actes communicationnels des utilisateurs à la manière de « coutumes » numérisées. En ce qu'il permet la rencontre de plusieurs expressions, internet constituerait un « lieu d'échanges », un espace communicationnel. Plus précisément, il conférerait aux utilisateurs l'aptitude d'énoncer/élaborer des règles selon les modalités offertes par le moyen de communication numérique – lequel livrerait un espace normatif horizontal, immédiat, décentralisé, hétérarchique²⁵⁷ –, donc distinctes des modalités offertes par le moyen de communication urbain – qui, toujours d'après une position habermassienne, aurait enfanté l'État comme organisation sociale verticale, mandatée, centralisée et hiérarchique.

Fut alors opposée une « démocratie étatique » (qu'elle soit représentative, participative, « continue »²⁵⁸...) à la « démocratie internet ». La première prend traditionnellement place dans

255 Par ex., en sciences politiques : ARSÈNE Séverine, *Internet et politique en Chine. Les contours normatifs de la contestation*, Karthala, 2011. En sciences de la communication : SHIRKY Clay, *Here Comes Everybody: How Change Happens when People Come Together*, Penguin, 2008 ; GERBAUDO Paolo, *Tweets and the Streets: Social Media and Contemporary Activism*, Pluto, 2012.

256 Par ex. en sociologie des usages : HARVEY Pierre-Léonard, *La démocratie occulte. Rapports de force, gouvernance et communautaire dans la société de l'information*, Presses de l'Université Laval, 2004, p. 17 : « si l'aphorisme le plus connu de McLuhan est "le médium, c'est le message" qui traduit un déterminisme technologique sur nos perceptions culturelles, on a occulté une autre de ses intuitions les plus importantes à l'ère de l'ordinateur : "le contenu c'est l'utilisateur" ». De quoi il déduit la formation de « tribus »/communautés d'utilisateurs dont le cadre d'existence serait conditionné par des capacités communicationnelles libérées des contraintes spatio-temporelles géographiques.

257 (i) Horizontal : le pouvoir d'élaborer des règles serait égal dans la mesure où chacun possède technologiquement les mêmes capacités communicationnelles (DUONG Lê-My, « Les sources du droit d'internet : du modèle pyramidal au modèle en réseau », *Recueil Dalloz*, p. 789-189). (ii) Immédiat : le pouvoir d'élaborer des règles ne s'exprimerait pas à travers un médiateur humain (législateur, juge...) mais serait directement exprimé par l'auteur de la communication ; ce pouvoir s'exercerait donc au rythme ininterrompu des communications en ligne à la différence du processus législatif étatique (PAUL Christian, Rapport « Du droit et des libertés sur l'internet », 2000, p. 16-17 : « Le temps du législateur ou du juge n'est pas et ne peut généralement pas être celui de l'internet. Si les institutions démocratiques veulent remplir leur rôle sans se trouver court-circuitées par la réalité, elles doivent être capables de traiter les questions posées avec la rapidité et la pertinence nécessaires. (...) La corégulation doit s'appliquer à permettre la rencontre difficile entre le temps de l'internet et le temps des institutions. »). (iii) Décentralisé : le pouvoir d'élaborer des règles serait non appropriable par une autorité centrale mais ouvert à toute personne désireuse de l'exercer (BERTHOU Renaud, « La démocratie électronique ou l'Internet et l'évolution de la participation des agents politiques à la prise de décision dans l'ordre juridique étatique », sur *marsouin.org*, 2002, cité par BERTHOU Renaud « La "forumisation" du droit : à propos des perspectives et enseignements d'une expérience originale de création du droit », *Droit et Société*, n° 61, 2005, p. 783-816 : « La communauté des internautes peut être appréhendée comme un ordre juridique »). (iv) Hétérarchique : le pouvoir d'élaborer des règles ne ressortirait d'aucune autorité supérieure dont serait tributaire les utilisateurs (BARRAUD Boris, *Repenser la pyramide des normes à l'ère des réseaux. Pour une conception pragmatique du droit*, L'Harmattan, 2012).

258 Issue de la Justice constitutionnelle qui en garantirait l'existence, cette démocratie continue théorisée par Dominique Rousseau admettrait l'« écart plutôt que la fusion » (est accepté que les actes du représentant puissent contrarier les droits constitutionnels du représenté), « la délibération et non la révélation » (ces droits du représenté sont assurés par la délibération du juge et non par une révélation

un environnement urbain où la communication interhumaine est spatialement et temporellement empêchée par l'éloignement physique ; la communication collective, simultanée et instantanée y étant impossible à grande échelle géographique, une parole devrait se singulariser des autres pour s'imposer collectivement, les citoyens devraient réserver à la collectivité une expression *distincte* pour que ses membres et exécutants soient en mesure de *distinguer* les règles énoncées par cette collectivité. La seconde prend place dans un environnement numérique où la communication interhumaine n'est pas spatialement ni temporellement empêchée par l'éloignement physique ; la communication y étant égalisée sans être empêchée, les internautes pourraient tout aussi également élaborer des règles, produire des normes et ainsi contribuer à un ordre normatif par « *auto-organisation* »²⁵⁹ indépendamment de l'échelle du réseau.

Afin d'éviter un conflit entre ces démocraties dans l'esprit du citoyen-internaute, ont été proposées par des constitutionnalistes l'extension du vote électronique, l'instauration d'un Parlement électronique, la participation citoyenne à la production normative (pétitions, amendements citoyens), une Charte des droits numériques insérée dans la Constitution²⁶⁰... Pour autant, d'une part, si les moyens matériels d'un acteur (comme un État par le recrutement d'agents, la création de faux comptes et la maximisation des relais communicationnels) lui permettent de contribuer abondamment à la diffusion de règles comportementales (comme la Russie ayant mis sur pied des *trolls farms* dont les employés rémunérés par la Fédération étaient chargés de favoriser l'élection de Donald Trump en 2016²⁶¹), la formation des règles en ligne peut-elle être observée comme issue d'un pouvoir communicationnel « égal » ? Si des communautés d'internautes se coordonnent pour étendre la visibilité d'un contenu au détriment des autres (comme des militants de La République En Marche ou de l'ex-Front National dont les *tweets* auraient recueilli, sur une période évaluée, un « coefficient de manipulation du trafic Twitter » très supérieur à la moyenne, i.e. auraient généré un trafic de données sur Twitter largement disproportionné par rapport au nombre d'utilisateurs impliqués²⁶²), la « démocratie internet » ne relèverait-

indiscutable car nationale, venue du législateur), « *les citoyens et non l'Etat* » (une telle démocratie repose donc sur la protection des droits des citoyens et non sur la parole de l'Etat). Pierre Brunet observe toutefois la relativité du lien entre « démocratie » et « justice constitutionnelle » : dire de la justice constitutionnelle qu'elle serait démocratique, i.e. qu'elle exprimerait la souveraineté populaire, c'est simplement dire que cette souveraineté du peuple est incarnée par la parole du juge au lieu de l'être par celle du législateur, qu'elle passe d'une main à l'autre. Ce passage de main n'implique pas nécessairement une « meilleure » garantie de la souveraineté du peuple, une « *meilleure démocratie* » comme le soutient D. Rousseau. Sur ce débat, v. BRUNET Pierre, « La démocratie, entre essence et expérience. Réponse à Dominique Rousseau », *La Vie des idées*, 2008 [en ligne]

259CARDON Dominique, *La démocratie Internet*, Seuil-La République des Idées, 2010, p. 85

260Sur un Parlement électronique, LE BOT Olivier, « Le vote électronique : modalités, potentialités, dangers » in LE BOT O. et ARLETTAZ J. (dir.), *La démocratie en un clic ?*, préc., L'Harmattan, 2010, p. 57. Sur la participation citoyenne, v. la synthèse de BONNET Julien et TÜRK Pauline, « Le numérique : un défi pour le droit constitutionnel », *Les NCC*, n° 57, 2017, p. 13-24. Sur une charte constitutionnelle, ROQUES-BONNET Marie-Charlotte, *Le droit peut-il ignorer la révolution numérique ?*, Thèse de droit, Michalon, 2010, p. 386-566

²⁶¹ PERROTTE Derek, « Visite guidée d'une "ferme à trolls" russe » [en ligne], *Les Echos*, 2018 ; PARIS Gilles, « Comment des "trolls" russes ont réussi à peser sur l'élection présidentielle américaine » [en ligne], *Le Monde*, 2018. Diverses ONG et enquêtes journalistiques estiment qu'il existe au moins une trentaine de *trolls farms* dans le monde.

²⁶² Le calcul de ce coefficient est permis par un algorithme né des travaux de l'*Oxford Internet Institute* suivant trois critères : (i) le nombre moyen de tweets par compte ; (ii) la proportion de retweets dans le trafic total ; (iii) le nombre de tweets des cinquante comptes les plus actifs. Conçu

elle pas plutôt d'un quasi-état de nature où le plus fort, le mieux organisé, le mieux équipé l'emporte sur les autres ? La démocratie ne serait-elle pas une « pratique » parmi d'autres du pouvoir communicationnel en ligne plutôt qu'une « nature » d'internet ? D'autre part, ceux des chercheurs qui prêtent une normativité à de telles « actions » communicationnelles tout en admettant la validité du CodIL en arrivent à la conclusion que nous avons soulignée au paragraphe précédent d'une aliénation plus ou moins déterminante des utilisateurs par rapport au code source²⁶³. Au vu de ces travaux et analyses scientifiques, le pouvoir des utilisateurs semble très relatif sur le plan communicationnel en comparaison du pouvoir des concepteurs.

B) Autres normativités identifiées en ligne

Deux principaux foyers de normativité ont été ciblés par la combinaison de la conception endogène (ordre normatif interne au réseau) **et de l'approche communicationnelle : les concepteurs maîtres du code source ; et, dans une mesure à la fois relative et dépendante de ces derniers, les utilisateurs** dont les expressions en ligne pourraient co-contribuer à façonner des règles comportementales. Des foyers normatifs supplémentaires ont été décrits lors de nouvelles combinaisons des enseignements endogènes et exogènes.

Premièrement, certains auteurs ont soumis l'axe hardwariste (notamment dans son approche « protocolaire », par couches) à des questionnements endogènes pour vérifier si des rapports normatifs se dégagent de l'architecture du réseau. Aux couches protocolaires du fonctionnement technique d'internet, Y. Benkler y fait correspondre trois couches empiriques

pour détecter le recours à des botnets (« *comptes-robots automatisés* ») et à des « cyborgs » (« *comptes-robots semi-automatisés qui présentent certains traits de comportement humains mais qui affichent une fréquence de production semblable à celle des machines* »), l'outil rendu public en 2019 avait déjà été utilisé pour mesurer divers hashtags (#StopAutoturfing, #4thofJuly) et tendances Twitter (Covfefe), et avait par ailleurs permis de constater une nette manipulation du trafic Twitter par les militants du Front National durant l'élection présidentielle de 2017 : NIMMO Ben, « Measuring Traffic Manipulation on Twitter » [en ligne], *Oxford Internet Institute*. Cet outil a ensuite été appliqué par l'ingénieur et hacker français Baptiste Robert sur la période 29 mars-1^{er} avril 2019 durant laquelle il relève, auprès de la communauté revendiquée La République En Marche sur Twitter et en soutien à leur candidate Nathalie Loiseau pour les élections européennes, un doublement du coefficient de manipulation du trafic par rapport à la moyenne : DELACROIX Géraldine et ROUGET Antton, « Comment une nébuleuse LREM instrumentalise les réseaux sociaux » [en ligne], *Mediapart*, 2019

²⁶³ Par ex., en droit : TÜRK Pauline, « Définition et enjeux de la souveraineté numérique », sur *Vie-publique.fr*, 2020 : « *nos sociétés deviennent dépendantes de la technologie et des entreprises qui les contrôlent (...), une tendance qui s'accroît avec le développement des algorithmes, des objets connectés, de la robotique, de l'IA. Or, ces technologies sont régies par le code informatique : dans l'espace numérique, la régulation des activités et comportements dépend davantage des standards et normes techniques déterminés par les ingénieurs informatiques que des normes juridiques édictées par les Etats. C'est le sens de la fameuse formule "code is law" de Lawrence Lessig* ». En sciences politiques : ARSÈNE Séverine, « Vers une recomposition des pouvoirs : Internet et réseaux sociaux », *CERISCOPE Puissance*, 2013 [en ligne], notam. §27s. En sociologie : CARDON Dominique, *La démocratie Internet*, préc., Seuil, 2010, p. 95-97 ; BADOUARD Romain, *Les Nouvelles Lois du web*, Seuil-La République des Idées 2020. En sociologie des usages : HARVEY Pierre-Léonard, *Design communautaire appliqué aux systèmes sociaux numériques. Fondements communicationnels, théories et méthodologies*, Presses de l'Université du Québec, 2014 (où l'utilisateur ne pourrait pleinement recouvrer son pouvoir communicationnel qu'en participant au *design* de la technologie)

pour en synthétiser le fonctionnement géopolitique²⁶⁴. La première couche qu'il appelle « physique » incorporerait les seules composantes matérielles du réseau (branchement câbles/terminaux, commutateurs, routeurs, antennes-relais, bornes wifi...), sa régulation établirait les conditions de transport de l'information (neutralité du Net, numérisation connectée de la télévision, passage à la 5G...). La deuxième couche qu'il appelle « logique » comporterait les éléments logiciels exécutés par le matériel (protocoles, adresses, systèmes d'exploitations, applis, sites web, programmes locaux...), sa régulation établirait les conditions de transformation de l'information (protection des droits d'auteur via des DRM, censure des informations illicites par les hébergeurs et éditeurs, *Privacy By Design* dans son versant logiciel, limitation du chiffrement...). La troisième couche « des contenus » engloberait toutes les données produites par les utilisateurs, sa régulation établirait les conditions d'utilisation de l'information (protection des consommateurs, commercialisation des informations...).

Approfondissant chacun de ces trois « niveaux de pouvoir » d'internet, Aurélien Bamdé tient le premier d'entre eux (physique) pour soubassement d'un « *ordre normatif numérique* ». L'architecture matérielle d'internet instituerait le cadre technique *au-delà duquel* ne peuvent agir les acteurs d'internet, et *dans lequel* s'insèrent les principes de fonctionnement fondamentaux interprétés par les usages de ces acteurs. Dès ses origines, l'architecture d'internet repose : (i) sur une structure maillée dans laquelle l'acheminement des adresses IP par les routeurs aurait été interprété par certains marchands comme la possibilité de recouper les données captées avec ces adresses IP devenues identifiantes malgré elles, assujettissant ainsi un large tronçon de la vie privée en ligne à des décisions commerciales ; (ii) sur un principe *end-to-end* qui, pour ne pas encombrer les équipements internes au réseau tels les serveurs et infrastructures, disperse les nécessités de calcul vers les terminaux en bordure du réseau, de quoi il résulterait un principe de neutralité inhérent au TCP/IP ; (iii) sur une interdépendance des couches qui conduit les acteurs de couches différentes et de même couche à élaborer puis à respecter des modalités d'interopérabilité suivant des normes, comme le service DNS mobilisé entre autres pour garantir l'interopérabilité des couches 3 et 7 et dont l'exploitation par l'Icann produirait de nouvelles normes²⁶⁵. Toute norme « interne » au réseau (décisions commerciales, principe de neutralité pour les intermédiaires du réseau, gestion par l'Icann...) dériverait primitivement des principes architecturaux portés par la couche physique et interprétés par les acteurs d'internet, y compris les internautes²⁶⁶. Dans leur éparpillement, ces normes qui procèdent d'un conditionnement matériel composeraient l'« *ordre normatif spontané* »²⁶⁷ du réseau internet auquel se heurte la régulation juridique. C'est dans la couche logique, où se transforment les informations, que le droit étatique pourrait agir efficacement (par ex., en collaborant activement aux activités et à la régulation du nommage DNS ou en enserrant la liberté de produire sur le Web des hyperliens

264BENKLER Yochai, « From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access », *Federal Communications Law Journal*, vol. 52, 2000, p. 561-579

265BAMDÉ Aurélien, *L'architecture normative du réseau internet.*, préc., 2014, p. 411s. (pour le premier exemple), p. 68-72 (pour le deuxième) et p. 399s. (pour le troisième)

266Ibid., p. 348 : « *les normes qui constituent [l'ordre numérique] ne sont autres que le fruit de l'interprétation (...) des principes architecturaux du réseau* ». On regardera toutefois cette explication comme manquant de cohérence dès lors que les principes architecturaux intègrent la couche logique (les protocoles), dont la couche physique est l'exécutante complémentaire. Ces deux couches étant indissociables sur le plan des principes architecturaux, on ne comprend pas pourquoi tenir l'une des deux pour fondamentale sur ce même plan.

267 Ibid., p. 241

attentatoires aux droits d'auteur ou à l'ordre public²⁶⁸). L'ordre numérique serait alors pénétrable par l'ordre juridique à travers les couches de fonctionnement du réseau. **Cette combinaison endo-hardwariste localise le foyer normatif dans l'usage de ces couches** comme acte positif d'interprétation de leurs principes architecturaux.

Deuxièmement, plus nombreux sont ceux qui combinent regard pragmatique et leçons endogènes. L'un des premiers a d'ailleurs été L. Lessig, qui dénombre quatre modes de régulation sont communément valables pour le cyberspace et l'espace urbain : l'architecture (l'environnement naturel en milieu urbain, le code source dans le cyberspace) ; les lois du marché ; les normes sociales²⁶⁹ ; et le Droit. Outre le « code », les trois autres modes de régulation sont donc extérieurs au réseau ; mais surtout, ils rappellent l'appartenance de l'acteur d'internet à la société humaine conformément à l'approche pragmatique. Sous cet éclairage, considérer le code source comme la source du pouvoir à l'intérieur du réseau est tout à fait compatible avec la constatation que d'autres sources de pouvoir sont pratiquées par des acteurs à l'extérieur du réseau depuis leurs activités. Plus encore, ces pouvoirs interne et externe interagiraient : la rédaction du code servirait l'activité extérieure ; et l'activité serait numériquement mise en œuvre par le code source. L'explication CodIL mit ainsi la lumière sur la neutralité fictive d'acteurs longtemps ramenés à de simples « intermédiaires techniques », mais dont les pratiques concilieraient en fait le *code-source* de leur logiciel et les *intérêts* de leur activité.

Cette conciliation a prioritairement été observée dans les pratiques algorithmiques. On a vu que les algorithmes pouvaient remplir diverses fonctions (analyse, validation, tri...) et en articuler plusieurs (modération...). La fonction remplie par l'algorithme de profilage consiste à associer un « double » (un « profil ») à l'internaute dont les habitudes, réactions, opinions, intérêts... sont extraits depuis les données collectées, *i.e.* depuis les données réceptionnées par le serveur et dont une copie est sauvegardée dans la mémoire du serveur²⁷⁰. Le profil ainsi obtenu peut être : exploité pour y adapter un service selon une clientèle-cible (modification du *design*, des prestations proposées, des prévisions budgétaires, du modèle économique...) ; monnayé auprès d'entreprises désireuses d'ajuster leurs services et produits aux intérêts du consommateur, ou encore auprès de « courtiers de données » (*data brokers* comme Axciom, Experian, LexisNexis,...) qui négocient la revente des données à d'autres entreprises ; vendu à des annonceurs pour dimensionner leurs publicités selon les attentes détectées (l'envoi de publicités sera ensuite individualisable à l'aide

²⁶⁸ *Ibid.*, v. le Titre 2 de la thèse, p. 339-550

²⁶⁹ L. Lessig n'est pas un penseur de la normativité au sens où on peut l'entendre en Europe et aborde assez approximativement ce concept. Il rapporte les normes sociales à des contraintes qui, collectivement déterminées par les membres d'une société humaine, imprègnent ces derniers « *d'une façon si familière qu'elle en est presque invisible* » (le langage, la civilité, la décence...) (LESSIG L., *Code: Version 2.0*, Basic Books, 2006, p. 11). Différentes de celles régissant l'espace physique (*ibid.* p. 19), les normes sociales du cyberspace résulteraient donc de l'action collective de ses membres, au premier rang desquels les internautes. En ce sens, le code-source ne serait pas en lui-même constitutif mais générateur de normes.

²⁷⁰ Généralement, le serveur web qui réceptionne directement les requêtes des internautes lui étant adressées transfère ces données vers des serveurs *ad hoc* à des fins de collecte, dotés d'une capacité de stockage spécifiquement élevée par virtualisation de la mémoire (simulation logicielle des capacités de la mémoire), et parfois entreposés dans des bâtiments (*datacenters*). Les données ainsi collectées sont parfois rangées dans des bases de données (*datawarehouse*) réutilisables pour les algorithmes.

d'algorithmes de personnalisation qui trient les annonces pertinentes selon le profil de l'utilisateur)²⁷¹ etc. Le profilage et la personnalisation algorithmique aboliraient la « moyenne » comme référence normative (opposant une majorité incluse dans la moyenne à une minorité exclue) au bénéfice d'une référence normative qui particularise le réel (opposant une « vérité numérique » à des vérités personnelles)²⁷². Les juristes Jean-Pierre Mignard et Adrien Basdevant reprennent explicitement la démonstration d'A. Rouvroy et T. Berns pour en déduire l'effet normatif d'un « oracle »²⁷³ incontesté (voire incontestable²⁷⁴) renvoyé par l'algorithme. Les algorithmes représenteraient alors le moyen économique de valorisation des données pour les activités commerciales autant que le moyen normatif de manipulation socio-cognitive, nécessitant une « régulation des algorithmes »²⁷⁵.

Outre les pratiques algorithmiques, celles contractuelles laissent à leur tour entrevoir un lien entre le code source et l'activité concernée. Lorsque plusieurs acteurs exercent un pouvoir exclusif sur le code source de leur logiciel, l'étendue de leur pouvoir semble varier selon les rapports contractuels de chacun. Les chercheurs en sciences de l'information et de la communication Marc Bassoni et Félix Weygand isolent le cas de la start-up berlinoise Aka'aki, fournisseuse d'un petit réseau social qui met en relation des comptes ouvertement géolocalisés afin que les rencontres en ligne provoquent des rencontres hors-ligne. Pour être attractive tout en économisant la recherche d'utilisateurs et annonceurs, la *start-up* aux faibles moyens est financièrement contrainte de passer par un prestataire de services déjà muni d'une vaste clientèle (Apple, Facebook, Google...). En l'espèce, elle a fait le choix de passer par Apple (en réservant l'accessibilité d'un jeu promouvant le réseau social aux utilisateurs d'*iPhone* et en déposant l'appli correspondante sur l'*AppStore*) et par Facebook (en requérant une connexion depuis un compte *Facebook* pour jouer). *Aka'aki* est contractuellement soumise à des « partenaires dominants » (Apple et Facebook), domination qui résulte de ce que « si Aka'aki trouve son marché et engrange des revenus, Apple prélève une commission ; si Aka'aki échoue (il s'agit de toute façon d'un partenaire de niche parmi une multitude), sa disparition n'aura pas d'influence perceptible sur la rentabilité globale d'Apple. Un partenaire domine tellement l'autre qu'il ne peut y avoir entre eux que des relations de collaboration »²⁷⁶. Inversement, la relation entre Apple et Facebook est régie par une « coopération » qui, tantôt positionnera ces acteurs en concurrents (pour la captation du temps limité d'attention des utilisateurs, le partage du pouvoir d'achat des utilisateurs prêts à payer pour l'accès aux services...), tantôt en fera des alliés contre Google (en limitant l'interopérabilité avec certains des

²⁷¹ Nous reprenons là des pratiques abondamment décrites et approfondies en sciences sociales, très bien synthétisées par BASDEVANT Adrien et MIGNARD Jean-Pierre, *L'Empire des données*, Don Quichotte, 2018

²⁷²*Ibid.*, p. 60s.

²⁷³*Ibid.*, p. 72. Marie-Anne Frison-Roche adhère également à cette approche du double numérique et en déduit que le temps se fige si, par prédiction ou par reproduction algorithmiques, le futur devient le présent sur la base du passé : FRISON-ROCHE M.-A., « Les conséquences régulatrices d'un monde repensé à partir de la notion de "données" », in M.-A. FRISON-ROCHE (dir.) *Internet, espace d'interrégulation*, préc., Dalloz, 2016, p. 207

²⁷⁴Par ex., si l'algorithme est opaque (PASQUALE Frank, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015), s'il a déjà produit des effets inaltérables à l'appui de cette vérité, si les résultats ou le processus décisionnel sont connus mais impossibles à remettre en cause (*Weapon of Math Destruction*)...

²⁷⁵BASDEVANT A. et MIGNARD J.-P., *L'Empire des données*, préc., 2018, p. 91s.

²⁷⁶BASSONI Marc et WEYGAND Félix, « Un jeu mobile, vecteur de "coopétition" entre réseau social numérique et *smartphone* » in AGOSTINELLI S., AUGÉY D. et LAURIE F. (dir.), *La richesse des réseaux numériques*, préc., Presses Universitaires d'Aix-Marseille, 2012, p. 67

services de Google comme *Gmail* par Facebook et le *PlayStore* pour Apple). De telles observations, certes datant de 2010 mais toujours valables en 2021²⁷⁷, amènent à relativiser le déterminisme de la maîtrise du code dans les rapports de force en ligne, puisque les relations contractuelles assoient le caractère plus ou moins indispensables de quatre acteurs (Aka'aki, Apple, Facebook, Google) pourtant chacun maître du code source de ses logiciels.

Les pratiques de *design*, enfin, révèlent un mouvement contraire par lequel des relations contractuelles dépendent du code source. Ainsi : la protection en ligne des entreprises et marques est tributaire de la manière dont les réseaux sociaux s'autorégulent²⁷⁸ (sanctions contre certains comptes parodiques, propos outranciers ou diffamatoires contre une entreprise, dispositifs de protection des droits d'auteur...) ; les modalités de diffusion d'annonces relèvent de contrats en grande partie déterminés selon les espaces publicitaires dédiés et loués par les annonceurs ; les conditions d'utilisation souscrites par les utilisateurs énoncent souvent des règles mises en œuvre par algorithme ou contenues dans les fonctionnalités ; les partenariats conclus entre les agrégateurs d'actualité, les réseaux sociaux et la presse pour augmenter la visibilité de cette dernière se concrétisent par des modifications du *design*... Qu'elle étudie les pratiques algorithmiques, contractuelles ou de *design*, **cette combinaison endo-pragmatique rend compte de foyers normatifs** (pour les rapports de force en ligne) **situés dans les pratiques des acteurs d'internet telles qu'elles relient leurs activités à leur code-source.**

Troisièmement, lorsque la donnée est étudiée en qualité d'information-bien, des enjeux propriétaires se dessinent comme « propres » au cyberspace. Du fait de la *peer-production* théorisée par Y. Benkler et qui ferait des « *individus les contributeurs de la construction d'un produit de travail de valeur en échange d'une reconnaissance ou d'une réputation* », un « *ordre social en ligne* » se distinguerait comme un « *précieux produit de [ce] travail* » collaboratif²⁷⁹. Au soutien de cette analyse, David Johnson, Susan Crawford et John Palfrey réclament que ce produit revienne à celles et ceux qui le produisent *via* leurs informations. Ils proposent dans cette direction que les machines ne puissent interagir qu'après leur validation par les utilisateurs. De cette manière, l'utilisateur aurait son enclos relationnel, choisirait les personnes « *de confiance* » avec lesquelles se connecter. Par interconnexion des divers cercles de confiance, les utilisateurs seraient ainsi protégés des cyberattaques²⁸⁰ : chacun aurait sa

277Pour un exemple actuel de « micro-réseau social » dépendant d'un autre plus grand, on citera CuriousCat adossé à Twitter ; pour la coopération, v. MARTY Frédéric, « Accès aux données, coopération intra-plateforme et concurrence inter-plateformes numériques », *Revue d'économie industrielle*, 2020, n° 169, p. 221-246

278MARTIN-BARITEAU Florian, « Les *Vanity URLs* : nouveaux enjeux et nouveaux risques pour les marques sur les réseaux sociaux » in AGOSTINELLI S., AUGÉY D. et LAURIE F. (dir.), *La richesse des réseaux numériques*, préc., 2012, p. 196s.

279JOHNSON David, CRAWFORD Susan et PALFREY John, « The Accountable Internet », *Virginia Journal of Law & Technology*, vol. 9, 2004, p. 7, note de bas-de-page n° 10

280Une telle issue nous semble toutefois inatteignable par ces propositions, y compris à l'époque de leur formulation, dès lors qu'un utilisateur ne télécharge pas volontairement ni consciemment une cyberattaque – le logiciel malveillant peut par exemple être téléchargé depuis une clé USB insérée par une tierce personne dans la machine du propriétaire (cas du virus Flame), ou depuis un hyperlien sur le Web dont le clic activera le téléchargement ; la cyberattaque peut par ailleurs circuler sans s'exprimer pour prendre le contrôle d'une masse de machines (*botnet*), et les cyberattaques peuvent au surplus viser des infrastructures-réseau (routeurs...) ou des services indispensables (serveurs DNS...) auxquels ils ont nécessairement accès pour se connecter à internet. Même à supposer qu'aucune

« *propre version d'Internet* », pourrait plus aisément discerner le licite (dans les cercles de confiance) et l'illicite (hors des cercles de confiance), garderait « *le contrôle du lieu virtuel sur lequel nous nous rendons en ligne et de qui (ou quoi) nous autorisons à faire partie de notre espace en ligne personnel* ». Ces cercles de confiance choisis et « responsables », où tout produit en ligne résulterait d'un travail collaboratif, correspondent à un schéma propriétaire à mi-chemin : du droit de propriété privée, développé pour garantir à son titulaire un espace matériel d'autonomie dont il peut pleinement et exclusivement jouir²⁸¹ ; et des *enclosures* britanniques du XVI^e siècle, instaurées pour réunir sous le joug du seigneur les biens communaux expropriés aux villageois²⁸². Une fois ses connexions validées par l'utilisateur dans son espace virtuel d'autonomie, les informations en ligne deviendraient, en raison d'une *peer-production* essentielle au réseau, inévitablement communes, exploitables par tous les membres validés de son cercle. **Suivant cette combinaison de la conception endogène et de l'approche économique de l'information, les rapports de pouvoir au sein du cyberspace** (« ordre social en ligne ») **seraient alors régis par les droits réels** (par opposition aux droits personnels) **qu'exercent les acteurs d'internet sur les informations**, soit pour en exclure des éléments indésirables (droits exclusifs comme le droit de propriété, les droits voisins, le droit de jouissance exclusive...), soit pour y inclure les éléments désirés (droit d'utilisation, droit d'accès, droits portant sur une servitude...).

En somme, les travaux jusqu'ici exposés ne l'ont évidemment pas été exhaustivement, mais les catégorisations théoriques dressées offrent une grille de lecture pédagogique qui nous semble couvrir les réflexions scientifiques les plus influentes dans l'analyse des rapports de force en ligne. Les enseignements endogènes et exogènes sont aujourd'hui plus souvent conjugués que conceptuellement opposés. Les divers angles de vue scientifiques ont permis d'identifier plusieurs foyers normatifs *dans* et *hors* du cyberspace, dévoilant des normativités croisées, régulées comme telles par le droit positif.

Paragraphe 2 - Le croisement de foyers normatifs juridiquement régulés

La conjonction des réflexions et conclusions scientifiques décrites a incliné la régulation d'internet par les États-Unis et l'Europe, visant les rôles (A) et pouvoirs (B) normatifs nouvellement identifiés.

A) De nouveaux rôles normatifs reconnus aux acteurs d'internet

D'une part, les analyses communicationnelles des rapports de force en ligne ont permis de préciser le rôle de certains acteurs pour les démocraties étatiques. Les conséquences normatives du pouvoir expressif des internautes s'affranchiraient d'une concentration de type étatique pour l'énonciation de règles collectives. On a vu que, pour certains auteurs, ce processus d'élaboration normative dit « en réseau » (*i.e.* hétérarchique, horizontal, décentralisé et immédiat) creuserait un écart entre la démocratie étatique et les usages démocratiques en ligne. L'une des

« personne de confiance » ne puisse devenir un cyberattaquant, un système sélectif tel que décrit ne pourrait protéger des cyberattaques.

281ROCHFELD Judith, Entrée « Accès », in CORNU Marie, ORSI Fabienne, ROCHFELD Judith (dir.), *Dictionnaire des biens communs*, PUF, 2017, p. 8 : « *La proclamation de la propriété exclusive est allée de pair avec un modèle d'autarcie matérielle pensé comme condition de la liberté individuelle reconnue* »

282GAUTHIER Florence, Entrée « Enclosure » in *ibid.*, p. 506-511

réactions privilégiées par l'État face à la crainte d'être déphasé fut d'adapter le mode d'élaboration du Droit.

Dès 1998, le Conseil d'État plaide pour la création d'un « *organisme de corégulation de l'Internet et des réseaux* » au « *fonctionnement souple* » qui institutionnaliserait un lieu de discussion entre acteurs publics et privés, afin d'ajuster la régulation selon l'évolution technologique en complément des obligations légales fixes de chacun (responsabilité des opérateurs/hébergeurs/éditeurs quant au privé, missions administratives quant au public)²⁸³. Dans son discours du 26 août 1999 tenu à Hourtin, le Premier Ministre Lionel Jospin entérine cette recommandation en s'appuyant sur les changements économiques et démocratiques apportés par le réseau internet²⁸⁴. Neuf mois plus tard, dans le cadre d'un rapport commandé par le Premier Ministre, le député Christian Paul fait des enjeux démocratiques et communicationnels le moteur de ce futur organisme en lui prêtant la forme d'un « *Forum* », plus précisément un Forum des droits de l'internet, après avoir estimé que « *l'internet nécessite de repenser la manière de « produire le droit »* »²⁸⁵. Avalisé par le Premier ministre en décembre 2000, le projet est mis sur pied en 2001 ; le droit étatique français officialise par-là son acceptation d'être élaboré « *de façon négocié* »²⁸⁶ sous l'effet d'internet. Les subventions versées par l'État n'étant plus renouvelées pour l'année 2011, le Forum des droits de l'internet disparut du même coup mais les expériences de co-élaboration du droit se sont poursuivies.

283Conseil d'Etat, Rapport « Internet et les réseaux numériques », 1998, p. 120 et 151s.

284JOSPIN Lionel, Déclaration sur la mise en œuvre et les orientations de développement du Programme d'action gouvernementale pour la société de l'information, 1999 : « *Le centre de gravité de l'activité économique se déplace, au point que se dessine ce que certains appellent une " nouvelle économie " . Si la formule est peut-être excessive, elle recouvre un changement bien réel dont le Gouvernement a pris la mesure. (...) Un Etat moderne est un Etat qui sait donner des impulsions sans se substituer aux acteurs de la société -citoyens, associations, entreprises, collectivités territoriales : l'Etat épaulé leurs efforts, en leur donnant les moyens d'agir par eux-mêmes. (...) Le réseau a en outre besoin d'une forme de régulation adaptée. Suivant en cela l'avis du Conseil d'Etat, le Gouvernement estime que la nature même de l'internet ne conduit pas à en confier la régulation à une autorité administrative indépendante spécifique. S'appuyant sur les expériences déjà menées en France et à l'étranger, qui mêlent régulation et auto-régulation, le Gouvernement proposera la mise en place d'un organisme qui associera, dans un but de concertation et de déontologie, acteurs publics et privés. »*

²⁸⁵ PAUL Christian, « Du droit et des libertés sur l'internet », préc., 2000, p.16-17 : le « *législateur ou [le] juge (...) nécessitent, pour être correctement instruits, la prise en compte d'éléments juridiques, économiques, technologiques, sociologiques (...) L'internet nécessite de repenser la manière de "produire le droit". (...) Si les institutions démocratiques veulent remplir leur rôle sans se trouver court-circuitées par la réalité, elles doivent être capables de traiter les questions posées avec la rapidité et la pertinence nécessaires. Elles doivent le faire en écoutant davantage, en collaborant mieux avec l'ensemble des acteurs et des parties prenantes aux débats. (...) La corégulation doit s'appliquer à permettre la rencontre difficile entre le temps de l'internet et le temps des institutions. Mais, à cette première dimension, s'ajoute la remise en cause des États-Nations par des réseaux mondiaux qui nient les frontières. Il serait hasardeux de formuler un pronostic sur l'issue de cette confrontation, même s'il est d'emblée permis de penser que la résistance aux "impératifs d'une société mondialisée intégrée au moyen du marché" (Habermas) est l'un des enjeux de ce temps. »* (les extraits soulignés l'ont été par l'auteur)

²⁸⁶BERTHOU Renaud, « La "forumisation" du droit : à propos des perspectives et enseignements d'une expérience originale de création du droit », préc., *Droit et société*, 2005, n° 61, p. 783

Depuis la révision constitutionnelle de 2008 ²⁸⁷, le pouvoir d'organiser un référendum n'appartient plus au seul Président de la République (référendum d'initiative présidentielle) mais également au Parlement, dont la proposition référendaire ne se concrétisera en référendum qu'après avoir obtenu le soutien d'un dixième du corps électoral dans un délai de 9 mois (référendum d'initiative partagée entre le Parlement et les électeurs). Le 6 décembre 2013, la loi organique n° 2013-1114 qui en détaille les modalités érige en principe le soutien par voie électronique (art. 5), et en exception celui par voie papier de toute façon enregistré sous format électronique pour sa comptabilisation (art. 6). Dans la même aspiration participative, la loi pour une République numérique (LRN) de 2016, du temps où elle n'était encore qu'un projet de loi, s'était enrichie d'« amendements-citoyens » déposables par tout citoyen français sur une plateforme y dédiée²⁸⁸. Au niveau local, les budgets participatifs, de plus en plus facilités par le recours au vote électronique et offrant aux habitants de contribuer à la répartition d'un montant du budget municipal, n'ont cessé de croître depuis 2014 en France²⁸⁹. Quelques tensions demeurent toutefois, et se renouvelleront sans doute, entre capacités numériques et démocratie étatique, rappelant que la seconde ne s'abandonne pas aux premières. Devenu sujet de discussion nationale porté par les Gilets Jaunes en 2018, un témoin récent de ces tensions a pris forme dans la revendication d'un référendum d'initiative citoyenne (désormais numériquement faisable) rejetée par les gouvernements français successifs depuis les années 2000 (pour y préférer un référendum d'initiative partagée électronisé).

Telles qu'identifiées, les conséquences du réseau numérique ont porté au point d'atteindre l'ordre juridique dans ses conditions d'existence (mode d'élaboration des règles de droit). En retour, l'accès au réseau internet est devenu une part intégrante de la démocratie juridiquement définie. On a déjà pu rappeler que le Conseil constitutionnel avait reconnu une liberté d'accès à un réseau de communications électroniques en 2009, ce au nom de « *la participation à la vie démocratique* »²⁹⁰. Outre-Atlantique, la Cour Suprême américaine avait déjà en 1997 justifié

287Loi constitutionnelle n° 2008-724 du 23 juil. 2008 de modernisation des institutions de la Ve République

288Compte-rendu du conseil des ministres du 9 déc. 2015 : « *Une concertation a d'abord été menée par le Conseil national du numérique, entre octobre 2014 et février 2015, conduisant à plus de 4 000 contributions qui ont inspiré la stratégie numérique du Gouvernement présentée le 18 juin dernier. Une relecture publique du projet a ensuite été organisée du 26 septembre au 18 octobre 2015, afin que celui-ci soit commenté et amendé en ligne. Ce processus a rassemblé des citoyens, des communautés qui se sont mobilisées sur une thématique particulière et des associations. Il a aussi vu la participation de nombreuses organisations professionnelles et d'entreprises. En seulement trois semaines, près de 21 000 participants ont publié 8 500 contributions. A l'issue de cet exercice, le Gouvernement a retenu cinq nouveaux articles d'inspiration citoyenne dans son projet et a intégré près de 90 modifications du projet. Cela démontre que la démarche collaborative peut contribuer à améliorer la participation politique des citoyens. Le Gouvernement a enfin répondu directement aux 250 contributions les plus populaires et ses réponses sont librement consultables sur la plateforme en ligne.* »

289Le nombre de communes engagées dans un budget participatif est passé de 7 à 138 au cours du mandat 2014-2020, doublant chaque année ; enquête nationale Budget participatif 2020 [en ligne sur lesbudgetsparticipatifs.fr]

290CC, *Hadopi 1*, 10 juin 2009, n° 2009-580 DC, cons. 12 : « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit [à la liberté d'expression] implique la liberté d'accéder à ces services* »

l'application de la liberté d'expression au réseau internet par l'accès qu'il autorise à de « vastes forums démocratiques »²⁹¹. En 2018, la Cour de district de New-York réitère ce précédent jurisprudentiel pour en déduire l'inconstitutionnalité du blocage sur Twitter, par le Président des États-Unis, de comptes pour des raisons de désaccord politique²⁹². Un tel blocage ayant pour effet d'invisibiliser les *tweets* du Président depuis les comptes ainsi bloqués, les victimes de cette pratique sont privées de l'accès à des actes « *qui ne peuvent être pris que le Président en qualité de Président* ». Le régime de la liberté d'expression n'étant pas le même pour un « *discours de gouvernement* » et un « *discours privé* », poursuit la décision, une responsabilité statutaire obligerait constitutionnellement le Gouvernement à ne pas discriminer l'accessibilité d'actes d'État selon les opinions politiques. Le blocage litigieux doit alors être vu comme contraire au Premier Amendement protégeant la liberté d'expression. Que soient étudiés les effets du réseau internet sur la construction démocratique du Droit²⁹³, ou au contraire l'intégration de ce réseau et de son accès dans la définition juridique de la démocratie, le droit constitutionnel positif accroît les droits des citoyens-internautes compte tenu du remaniement, par leur rôle communicationnel en ligne, des enjeux de la démocratie étatique.

D'autre part, parmi les foyers normatifs décelés à l'aide des travaux scientifiques et de leurs combinaisons, on a pu relever les utilisateurs mais aussi, en situation dominante par rapport aux premiers, les acteurs qui exercent un pouvoir sur le code-source (développeur, propriétaire ou détenteur du logiciel...). Ces analyses ont fait apparaître chez ces acteurs un caractère intentionnel (maîtrise du code) là où le droit positif voyait une neutralité fonctionnelle (hébergement de logiciels et de contenus). Or, comme c'est classiquement le cas en droit, la découverte de l'intention enclenche la compétence et aggrave la responsabilité ; les maîtres du code n'ont guère échappé à cette règle²⁹⁴.

C'est aux États-Unis que le *design* sera initialement utilisé comme critère déclencheur de la compétence du juge pour un litige impliquant un site web, aussi international qu'internet est accessible. En 1997, la Cour Suprême distingue trois catégories de sites selon la programmation de leur interface²⁹⁵ : (i) le site dont l'interface se contente de mettre à disposition des utilisateurs des informations tierces est dit « *passif* », et la juridiction compétente pour connaître de ses litiges est celle dans le ressort duquel se situe le fournisseur de contenu, *i.e.* le créateur du site ; (ii) le site dont l'interface établit un échange d'informations entre le serveur et le terminal utilisateur est dit « *interactif* », et la juridiction compétente en cas de litige dépendra du « *niveau d'interactivité et de la nature commerciale de l'échange d'informations* » ; (iii) le site sur lequel

291 Cour Suprême des États-Unis, *Reno v. ACLU*, 521 U.S. 844 (1997)

292 *Knight Institute v. Donald Trump*, No 17 Civ. 5205 (NRB) (S.D.N.Y. May 23, 2018)

293 V. l'ex. de la corédaction d'une révision constitutionnelle islandaise *via* la technologie en réseau : SALES Éric, « La transformation de l'écriture de la Constitution, l'exemple islandais », *Les NCC*, n° 57, 2017, p. 45-57

294 CHERIGNY Florence, « Conclusion générale » in CHERIGNY Florence et ZOLLINGER Alexandre, *Les objets connectés*, Presses universitaires juridiques, Université de Poitiers, p. 170 : « Bien loin d'être des objets inanimés, les objets connectés sont des objets programmés, animés par des intentions humaines, soulevant des difficultés d'analyse qui risquent de devenir essentielles au regard du dispositif de protection des données personnelles : comment aborder les finalités déterminées, légitimes et explicites [que tout traitement de données personnelles doit se fixer et respecter], alors que de tels objets peuvent être conçus pour des finalités aussi diverses, portées par de si nombreux acteurs ? »

295 *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. aux pts 1119-1123 (W.D. Pa. 1997)

l'achat d'un produit se fait exclusivement en ligne est dit « commercial », et toute juridiction dans le for duquel le site web est accessible est compétente. Cette jurisprudence sera longtemps dominante²⁹⁶, bien que d'autres méthodes aient été parallèlement usées pour arrêter la compétence du juge – le *targeting test* (le for compétent est celui vers lequel le site web dirige son activité) surtout recouru en matière civile²⁹⁷, et le « *blanket* »²⁹⁸ *test* (le for compétent est celui depuis lequel le site web est accessible) dans les autres cas.

En France et en Europe, le *design* sera moins regardé comme facteur de compétence que comme facteur de responsabilisation. En 2006, alors que l'ancienne rubrique « Liens Commerciaux » de Google renvoyait vers les publicités de sites web concurrents de Louis Vuitton chaque fois que cette marque était saisie dans le moteur de recherche, la Cour d'appel de Paris retient la responsabilité de Google pour son rôle actif dans l'organisation du *design* de son logiciel au service de son activité commerciale²⁹⁹. De cet argument endo-pragmatique (par les pratiques de la société Google, le code source est concilié avec les intérêts de son activité), la Cour d'appel en déduit qu'un tel rôle actif prive en l'espèce Google du statut d'hébergeur et de l'irresponsabilité de principe y assortie vis-à-vis des contenus hébergés. S'ensuit une jurisprudence équilibrée qui conditionne le bénéfice de ce statut selon un rôle « passif », dont l'absence de définition a pu mener à des dilemmes pour départager les divers rôles d'un même acteur³⁰⁰. Le critère sera repris en 2010 par la Cour de Justice de l'Union Européenne (CJUE)

296ROSS SUNHAM Catherine, « *Zippo-ing the Wrong Way : How the Internet Has Misdirected the Federal Courts in Their Personal Jurisdiction Analysis* », *University of San Francisco Law Review*, vol. 43, p. 559-584

297Issu de *Calder v. Jones*, 465 U.S. 783, 783-84 (1985), appliqué à internet depuis *GTE New Media Services Inc. v. BellSouth Corp.*, 199 F.3d 1343 (2d Cir. 2000)

298MATWYSHYN Andrea M., « *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction through Data Privacy* », vol. 98, *Northwestern Law Review*, p. 506. Ce test précède légèrement l'arrêt *Zippo* : *Inset Sys., Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996)

²⁹⁹ CA Paris, 4^e ch. Sect. A, *Google France c. Louis Vuitton*, 28 juin 2006 : « [Google France et Google Inc.] ne se bornent pas à stocker des informations de nature publicitaire qui lui seraient fournies par des annonceurs, mais (...) déploient une activité de régie publicitaire, d'abord, en organisant la rédaction des annonces, en décidant de leur présentation et de leur emplacement, ensuite, en mettant à la disposition des annonceurs des outils informatiques destinés à modifier la rédaction de ces annonces ou la sélection des mots clés qui permettront de faire apparaître ces annonces lors de l'interrogation du moteur de recherche et, enfin, en incitant les annonceurs à augmenter la redevance publicitaire coût par clic maximum pour améliorer la position de l'annonce ; (...) l'activité publicitaire ainsi déployée constitue l'essentiel du chiffre d'affaires réalisé par les sociétés appelantes qui, au mois de juillet 2004, annonçaient qu'au premier semestre 2004, 98% du chiffre d'affaires a été généré par les annonceurs publicitaires »

³⁰⁰Le service « AdWords » de Google – par lequel des annonceurs peuvent louer des mots-clés renvoyant vers des sites sponsorisés (premiers résultats de la page lorsque l'utilisateur saisit ces mots-clés), et auquel la Cour d'appel de Paris avait dénié le statut d'hébergeur en 2006 dans le cas *Louis Vuitton* – a été requalifié d'« hébergeur » en 2013 par la même Cour au motif que Google se contente de référencer une annonce créée par autrui (l'annonceur), alors pourtant que le *design* de Google était toujours aussi déterminant dans la présentation des annonces et que ses revenus provenaient toujours aussi essentiellement de la publicité : CA Paris, Pôle 2 ch. 7, *Google Ireland, Google France c. Olivier M.*, 11 déc. 2013. En 2010, la Cour de Cassation reconnaît la qualité d'hébergeur à Dailymotion dont le rôle serait principalement passif, tout en pointant les capacités de Dailymotion de refuser à ses membres l'accès à un espace personnel pour se réserver les vidéogrammes de cet espace « à titre exclusif », « modifier à tout moment les modalités de l'accessibilité à cet espace personnel »,

qui réserve l'irresponsabilité aux activités « *techniques, automatiques et passives* » d'hébergement³⁰¹. L'année suivante, jugeant qu'un même acteur (eBay) pouvait porter la double casquette d'hébergeur passif irresponsable (« *en stockant sur ses serveurs les offres à la vente, en fixant les modalités de son service, en étant rémunéré pour celui-ci et en donnant des renseignements d'ordre général à ses clients* ») et de commerçant actif responsable (« *en prêtant une assistance [aux commerçants en ligne] (...) consistant notamment à optimiser la présentation des offres à la vente en cause ou à promouvoir ces ventes* »)³⁰², la CJUE fonde la recherche de responsabilité non plus sur un statut indivisible d'un acteur mais sur le(s) rôle(s) que joue cet acteur en pratique *via* son *design* et ses recettes. Elle y clarifie un rôle actif caractérisé par une « *connaissance ou un contrôle des données stockées* » (pt. 6). Sur toute la décennie, la maîtrise du *design*, consubstantielle à toute activité logicielle, est peu à peu relativisée en tant que critère de responsabilisation, au profit de cet autre critère de la « *connaissance ou du contrôle des données* ». Ce glissement s'explique par découverte de pouvoirs chez des acteurs à la jonction de plusieurs foyers normatifs en ligne : les plateformes.

B) De nouveaux pouvoirs normatifs reconnus aux acteurs d'internet

Dès les années 2000³⁰³, une « plateforme » d'un réseau numérique est abordée comme un service ligne dont le principe consiste très simplement à mettre des utilisateurs en relation. Ce mode opératoire a principalement attiré l'attention des économistes, qui ont enrichi la signification associée aux plateformes. Les utilisateurs qu'elles relient peuvent être purement des consommateurs (plateforme C2C, comme les réseaux sociaux, les services de covoiturage ou de locations hors-bail de type Airbnb etc.), purement des professionnels (i.e. des personnes dont les activités économiques ou contractuelles habituelles s'inscrivent dans un cadre commercial, industriel, artisanal, libéral ou agricole³⁰⁴, avec le cas de plateformes B2B comme Alibaba, TradeKey, AmazonBusiness etc.), ou bien des professionnels en contact avec des consommateurs (plateformes B2C comme Amazon, eBay, PriceMinister, Uber, Rakuten, Deliveroo etc.). Dans les faits, il n'est pas rare qu'une même plateforme cumule des services de B2B, de B2C et de C2C (par ex., un moteur de recherche qui référence des hyperliens renvoyant vers des services commerciaux et des hyperliens renvoyant vers des blogs dits « amateurs », non-professionnels). Ce service commercial de mise en contact ferait germer un modèle économique biface, i.e. stimulant les relations entre deux groupes d'utilisateurs³⁰⁵ (par ex., les annonceurs ont intérêt à contacter les internautes pour la diffusion de publicités, les internautes ont intérêt à contacter leurs amis internautes pour leur lien social, ou à contacter des commerçants pour l'achat en ligne de vêtements...), voire multiface si plus de deux groupes sont raccordés par la plateforme³⁰⁶.

« *poster des commentaires* », « *créer les mots-clés permettant de référencer [un élément d'identification des contenus] au sein du moteur de recherche du service* » etc. : Cass., Civ. 1^e, 17 fév. 2011, n° 09-67.896. Ont encore été reconnus comme hébergeurs Wikipédia (TGI, ord., 29 oct. 2007), Facebook (TGI Paris, ord., 13 avr. 2010), Twitter (CA Paris, ord. 12 juin 2013), tandis qu'Alibaba aurait la qualité d'éditeur (le TGI Paris, ord. 21 nov. 2017 reprenant l'argument qu'on pensait abandonné du *design*, utilisé par la CA Paris, *Louis Vuitton*, 2006)

³⁰¹CJUE, Gde ch., *Google France c. LVMH*, 23 mars 2010, aff. C-236/08, pt. 113

³⁰²CJUE, Gde ch., *L'Oréal c. eBay*, 12 juil. 2011, aff. C-324/09, pts. 115-116

³⁰³Par ex., VON HIPPLE Eric, « Democratizing Innovation », *MIT Press*, 2005 (sur la manière dont les informations issues des interactions d'utilisateurs via une plateforme contribuent à l'innovation) [en ligne sur oecd.org]

³⁰⁴ Code de la consommation, art. liminaire

³⁰⁵ROCHET Jean-Charles et TIROLE Jean, « Platform competition in Two-sided Markets », *Journal of the European Economic Association*, vol. 1-4, 2003, p. 990-1029

³⁰⁶ PÉNARD Thierry et RALLET Alain, « De l'économie des réseaux aux services en réseaux », *Réseaux*, n° 184-185, 2014, note de bas-de-page n° 1

Les plateformes concentrent ainsi les échanges entre les divers groupes d'acteurs en ligne et, en cela, hébergent un grand nombre d'informations provenant de sources plurielles d'interactions. Or, si l'« information » partage certes les propriétés d'un « bien » économiquement appropriable, ce n'est pas un bien tout à fait ordinaire : il est dit « non-rival », c'est-à-dire que « *son usage par un individu ne limite pas la possibilité d'usage pour les autres, plusieurs individus pouvant ainsi utiliser simultanément ce bien (ou ce service)* »³⁰⁷. La non-rivalité de ce bien emporte une conséquence économique extrêmement avantageuse : si les coûts de production d'une information (par ex. la rémunération de développeurs pour la conception d'un logiciel, l'achat d'un terminal pour produire des données en ligne...) peuvent être élevés, ses coûts de reproduction sont très faibles voire quasi-nuls.

Une économie basée sur l'information rompt donc radicalement avec le modèle fordiste d'une économie industrielle basée sur la transformation de biens matériels rivaux. Dans le modèle fordiste en effet, les coûts de (re)production constituent une limite intrinsèque à l'obtention d'un monopole. Toute entreprise a des coûts fixes (invariants, tel le loyer d'un bail commercial) et des coûts de production (évolutifs). Si l'entreprise poursuit son activité à long terme, les coûts de production finiront à un moment par dépasser les coûts fixes. Ce moment franchi, les coûts fixes sont amortis et les coûts de production de chaque produit diminuent. Les économies ainsi réalisées par l'entreprise, dites « d'échelles », sont donc tirées par l'offre (donc la production). Or, l'offre est limitée : plus une entreprise produit, plus il lui faut organiser sa production (créer des règles, résoudre des dysfonctionnements etc.) ce qui engage des coûts exponentiellement élevés par rapport à la quantité produite, enrayant l'accès à un plein monopole³⁰⁸. Inversement, l'information étant non-rivale et sa reproduction peu coûteuse, la demande peut consommer des produits/services sans limite quantitative de l'offre ; le bien peut être consommé infiniment³⁰⁹. Une économie de l'information est alors tirée par la demande.

Les possibilités d'expansion économique sont alors sensiblement différentes dans ce nouveau contexte où « *tout ce qui peut être numérisé (...) est une information (...) pour laquelle des gens sont prêts à payer* »³¹⁰. Réceptacles d'un grand nombre d'informations du fait même de leur activité, les plateformes sont les premières bénéficiaires de ces nouvelles règles du jeu économique. Tirée par la demande, cette économie satisfait non plus aux lois de l'offre mais à celles de la consommation. Ici, la demande semble répondre à des « *effets de réseau* » (loi de Metcalfe) : plus une plateforme compterait d'adhérents, plus elle en obtiendrait de

307C'est encore le cas de l'air, de l'éclairage urbain, de la sécurité... v. WEINSTEIN Olivier, Entrée « Bien public (approche économique) » in CORNU M., ORSI F., ROCHFELD J. (dir.), *Dictionnaire des biens communs*, préc., PUF, 2017, p. 89

308(Sauf au moyen de pratiques contractuelles altérant l'état du marché comme des OPA, des rachats...) V. SHAPIRO Carl, VARIAN Hal R., *Information Rules*, Harvard Business School Press, 1999, p. 173 s.

309Le consommateur, lui, ne peut en revanche consommer que dans la mesure permise par sa capacité d'attention à l'information. Les fournisseurs de services en ligne au contact direct de l'utilisateur qui exploitent l'économie de l'information sur le réseau se concurrencent alors souvent sur un « marché de l'attention ».

310SHAPIRO Carl, VARIAN Hal R., *Information Rules*, préc. Harvard Business School Press, 1999, p. 3

supplémentaires³¹¹. La conjugaison (i) de la réduction du coût unitaire en fonction du volume de production, (ii) de l'apprentissage par la pratique et (iii) des externalités du réseau (*i.e.* des effets de réseau) produirait non plus des économies d'échelles, mais des « *rendements croissants d'adoption* » (RCA). Concrètement, plus les consommateurs adopteraient la technologie, plus elle gagnerait en performance, d'où le propriétaire de la technologie puiserait ces rendements croissants³¹². Les RCA conduiraient à ce qu'« *une technologie n'est pas choisie parce qu'elle est la meilleure, mais elle devient la meilleure parce qu'elle est choisie* »³¹³.

Cette structure de l'économie de l'information aboutirait à un cercle vicieux : une même plateforme attire sans cesse plus de d'adhérents (effet de réseau), donc augmente exponentiellement ses rendements (RCA), lui offrant ainsi d'améliorer son bien/service pour attirer plus de clients et ainsi de suite. **Le libre-jeu d'un marché basé sur l'exploitation commerciale de l'information en réseau aurait alors pour effet de fortifier des plateformes-oligopoles** (Facebook, Amazon, Apple...). La stimulation de la demande (utilisation financièrement gratuite de la plateforme, renchérissement des interactions entre groupes d'utilisateurs, captation de l'attention des internautes...) serait plus que jamais déterminante dans la concurrence entre plateformes pour optimiser le nombre et la qualité d'informations à valoriser économiquement. L'un des principaux leviers de l'économie de l'information résiderait alors dans le contrôle des « externalités », des éléments externes à l'autonomie de choix du consommateur (sa volonté) qui orientent l'état du marché. Lorsque la plateforme paramètre les conditions des communications qu'elle héberge, elle exerce un contrôle sur les interférences et interdépendances des utilisateurs, elle « *internalise* » ces externalités, renforçant de la sorte l'effet de réseau par la sujétion du consommateur aux externalités que génère la plateforme³¹⁴ (on a déjà cité l'exemple de la fonctionnalité « message lu/vu » sur les plateformes de messagerie instantanée qui suscite l'attente d'une réponse). Les sciences économiques de l'information en ligne rejoignent ici la sociologie des usages, puisque l'accaparement, l'« internalisation » des externalités serait source de « *prescriptions d'usage* » pilotant les comportements des utilisateurs dans un sens fixé par la/les personnes désireuses d'en tirer profit³¹⁵. De là a germé l'idée, parmi les

311Plus précisément, l'utilité d'un réseau serait proportionnelle au carré du nombre de ceux qui l'utilisent.

Elaborée empiriquement par Robert Metcalfe en 1980 sur la base d'interactions machinales prévisibles et répétitives, puis validée dans son application aux utilisateurs du réseau internet en 1993 par George Gilder, cette formule s'applique toutefois approximativement aux êtres dont l'activité est irrationnelle. Si l'exactitude mathématique est mise en doute, la réalité des effets de réseau a été plusieurs fois confirmée depuis : par ex., CURIEN Nicolas, FAUCHART Emmanuelle, LAFOND Gilbert, LAINÉ Jean, LESOURNE Jacques, MOREAU François, « Forums de consommation sur Internet. Un modèle évolutionniste », *Revue économique*, vol. 52, 2001, p. 122

312ARTHUR W. Brian, « Competing Technologies, Increasing Returns, and Lock-In by Historical Events », *The Economic Journal*, vol. 99, 1989, p. 116-131

313JOLLIVET Pascal, « Les rendements croissants », *Revue Multitudes*, n° 2, 2000, p. 95

314BENZONI Laurent et DUTRU Pascal, « De l'accès aux infrastructures à l'accès aux moyens numériques », in FRISON-ROCHE M.-A. (dir.), *Internet, espace d'interrégulation*, préc., Dalloz, 2016, p. 30s. Sur la manipulation de ces externalités par les plateformes à des fins économiques, v. ROCHELANDET Fabrice, *Économie des données personnelles et de la vie privée*, Repères, 2010, p. 38s.

315PAQUIENSÉGUY Françoise, « L'utilisateur et le consommateur à l'ère numérique », in G. VIDAL (dir.), *La sociologie des usages*, [supra note], 2012, p. 191-192 : « [L']offre industrielle (...) est antérieure à la formation des usages en ce sens qu'elle a une génération (...) d'avance sur les

chercheurs, que l'activité des utilisateurs s'apparenterait en fait à une activité de « travail » au profit des plateformes : les plateformes « recrutent » les utilisateurs (effets de réseau), influencent leurs comportements (prescriptions d'usage) et en tirent profit (RCA). Ce mouvement scientifique dénonçant un « *digital labor* » est synthétisé par la formule « *capitalisme cognitif* » venue de l'économiste Yann Moulier-Boutang et pointant le phénomène d'une valeur économique extraite de la contribution collective intellectuelle d'internautes non rétribués à ce titre³¹⁶. Au début de la décennie 2010³¹⁷, (i) les sociologues P.J. Rey (2012) et Antonio Casilli (2010 et 2014) militent pour que la puissance publique garantisse un partage équitable de cette valeur économique obtenue, (ii) tandis que l'informaticien-philosophe Jaron Lanier (2014) situe une partie du remède dans des micro-paiements versés à l'utilisateur en contrepartie de l'exploitation de son information³¹⁸, et (iii) que d'autres chercheurs en sciences sociales³¹⁹ se penchent sur l'hypothèse d'une diffusion de certaines informations en ligne (données personnelles, logiciels participatifs, données dont l'exploitation privative distord la libre concurrence, bases de données...) tels des « *biens communs* », des biens sur lesquels chacun pourrait exercer les mêmes droits réels et dont la transformation et la valorisation profiteraient *inclusivement* à tous les participants de ce travail collectif plutôt qu'*exclusivement* aux plateformes et leurs partenaires³²⁰.

utilisateurs. En matière de technologies de l'information et de la communication numérique, cette antériorité permet justement aux industriels et prestataires de services de s'adapter aux usages en cours, en saisissant l'usager comme témoin et expert de ses propres usages, présents comme anticipés. Si l'épaisseur de cette antériorité se réduit en même temps que les cycles de vie des produits, elle se renforce cependant car elle exploite directement, et autant que possible, le comportement des usagers pour construire des scénarios d'usages, des prescriptions d'usages dont certains fonctionnent sur la base d'une participation, d'une intégration des contenus et des actions des usagers dans les stratégies de l'offre. »

316MOULIER-BOUTANG Yann, *Le Capitalisme Cognitif : La Nouvelle Grande Transformation*, Amsterdam, 2008

317V. en détail ANCIAUX Arnaud, FARCHY Joëlle et MÉADEL Cécile, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* n° 158, 2017/2, p. 9-41

318Actualisant ainsi la proposition faite par l'informaticien Keneth C. Laudon en 1996 d'un « *prix de compensation* » pour l'achat ou la vente des informations en ligne : LAUDON Keneth C., « Markets and privacy », *Communications of the ACM*, 1996, p. 92-104

319Par ex., en économie : HESS Charlotte et OSTROM Elinor (dir.), *Understanding Knowledge as a Commons*, MIT Press, 2007 ; CORIAT Benjamin, « L'idéologie propriétaire a atteint ses limites », *Libération*, 2015 ; FARCHY Joëlle, « Numérique : "Il faut un écosystème de partage des données soutenable sur le long terme" », *Le Monde*, 2018. En droit : LESSIG Lawrence, *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, 2001 ; CLÉMENT-FONTAINE Mélanie, « Internet et la résurgence des communs » in PARANCE Béatrice et DE SAINT VICTOR Jacques (dir.), *Repenser les biens communs*, CNRS, 2014, p. 261s. ; ROCHFELD Judith et SICHEL Olivier, « Nos données nous appartiennent », *Le Monde*, 2015. En sociologie et socio-économie : BROCA Sébastien et CORIAT Benjamin, « Le logiciel libre et les communs », *Revue internationale de droit économique*, 2015, p. 265-284 ; CARDON Dominique, *Culture numérique*, Presses de Sciences Po, 2019, p. 111s.

320Par ex., en plaçant les données personnelles sous un régime de « biens communs » (*Biens communs : un circuit ouvert*, Juris associations, n° 501, 2014), ou au moyen plus privilégié de *Creative Commons* (licences développées par L. Lessig en 2001, par lesquelles l'auteur d'un logiciel cède tout droit de libre (ré)utilisation, modification, copie, diffusion publique, partage interindividuel... : ZIMMERMANN Jean-Benoît, « La musique à l'heure de l'Internet : du patrimoine aux communs ? » in CORIAT Benjamin (dir.), *Le retour des communs : la crise de l'idéologie propriétaire*, Les liens qui Libèrent, 2015)

Quel que soit l'angle scientifique adopté, études après études, foyers normatifs après foyers normatifs, les travaux scientifiques endogènes, exogènes et leurs combinaisons convergent dans leur majorité pour viser les plateformes comme titulaires d'un pouvoir particulièrement expansif en ligne. Elles maîtrisent le code source (CodIL) ; elles conditionnent les moyens de communication (approche (endo-)communicationnelle) ; leurs pratiques contractuelles les rendent prépondérantes et inévitables, leur clientèle est suffisamment étendue pour que leurs pratiques algorithmiques aient une large portée, elles exercent des droits réels de nature commerciale sur le plus grand nombre d'informations en ligne ((endo-)pragmatisme) ; elles en retirent une position économique dominante (approche économico-juridique de l'information comme bien).

Les producteurs et les exécutants du droit positif ont pris acte de ces conclusions. Dès 1998, le législateur américain appréhende partiellement l'activité des plateformes à travers la notion d'*Internet Information Location Tools* (ILT), qui se réfère à un service d'agrégation d'informations mis à disposition des internautes sur le Web³²¹. Les ILT ne sont pour autant devenus un profond levier d'action qu'après la démonstration de la centralité des plateformes dans les rapports de force en ligne. En mai 2011, le Sénat propose l'adoption d'un *PROTECT IP Act* (PIPA) qui prévoyait un dispositif de sanction administrative contre les sites web hébergeant des contrefaçons au sens du droit américain. Concrètement, sur délivrance préalable d'une ordonnance par un tribunal, les agents administratifs chargés d'exécuter la loi (police, services de renseignement...) pouvaient exiger³²² : à l'opérateur d'un serveur DNS d'empêcher l'accès au nom de domaine du site frauduleux ; au fournisseur de transaction financière (Visa, MasterCard...) de cesser la fourniture de ses moyens de paiement au site ; aux services de publicité de ne plus fournir d'annonces sur le site ; et aux ILT d'empêcher l'accès aux noms de domaine frauduleux (notamment par déréférencement sur les moteurs de recherche). En septembre 2011, la Maison Blanche propose un texte similaire au PIPA venant à son renfort, le *Stop Online Privacy Act* (SOPA). Comme leur prédécesseur de 2010, le *Combating Online Infringement and Counterfeits Act* (qui n'empruntait pas encore la voie des ILT pour la sanction), le PIPA/SOPA échouèrent sous la pression entre autres d'une vaste contestation sociale, la date de leur vote fut reportée *sine die*. En 2018, pour la première fois depuis le *Digital Millennium Copyright Act* (DMCA)³²³ de 1998, une nouvelle exception est ajoutée au régime d'irresponsabilité des hébergeurs. Cette irresponsabilité, introduite en 1996 par le *Communication Decency Act*, tombait dans trois cas – lorsque l'hébergeur ne retire pas rapidement une contrefaçon ou un contenu criminel lui ayant été signalés, ou lorsqu'il permet un accès non-autorisé (car atteignant la vie privée) à une communication qu'il héberge. Ajoutée en 2018 par l'*Allow States and Victims to Fight Online Sex Trafficking Act* (FOSTA), la quatrième exception engage la responsabilité de l'hébergeur qui accueille une annonce publicitaire promouvant la traite sexuelle des êtres humains (prostitution etc.), dans les mêmes conditions qu'est engageable la responsabilité de l'annonceur en cause.

Entraînant hébergeurs et ILT, une tendance à la responsabilisation légale affecte de plus en plus les acteurs qu'on appelle, en fait, « plateformes ». La même tendance s'observe en France

321Public Law 105-277 du 21 oct. 1998, Titre XI, Sect. 1101,(3)(E) : un ILT est « *un service qui renvoie ou relie les utilisateurs à un emplacement en ligne sur le World Wide Web. Ce terme comprend les répertoires, index, références, renvois par clics et liens hypertextes* » (Titre 47 du USCS §231 (chapitre 5))

322PIPA, Section 3 (d)(2)(B)

323Dont la section 512 prévoit l'exception relative aux contrefaçons

et en Europe, sous la forme plus explicite d'une « obligation légale de coopération avec des États » pesant sur les plateformes. Sur la première moitié des années 2010, le droit français redéfinit peu à peu les hébergeurs en co-exécutants du droit étatique, en « *collaborateurs nécessaires de la justice* », « *à la fois susceptibles de prendre part à la commission de l'infraction [en la faisant exister par l'hébergement] et à la lutte contre la cybercriminalité [par leurs obligations légales]* »³²⁴. Aussi longtemps qu'une illicéité en ligne n'est pas portée devant le juge, son sort relève, bien plus que de simples *pratiques* d'appréciation, d'une véritable *compétence* décisionnelle de l'hébergeur homologuée par le juge. Cette compétence est clairement retranscrite par deux ordonnances rendues le 6 octobre 2010 à Paris et à Lille. En l'espèce accusée d'héberger le service illicite *Wikileaks*, la société OVH spécialisée dans la location de ses serveurs ne pouvait invoquer son irresponsabilité de principe puisqu'elle avait indéniablement conscience du contenu infractionnel ; se déportant alors sur un autre terrain, elle soutient que la caractérisation de l'illicéité d'un contenu étant du ressort du juge, elle ne peut être tenue pour responsable d'avoir maintenu l'hébergement de *Wikileaks* en connaissance de cause. Le juge lui rétorque qu'il revient à l'hébergeur, « *hors de toute instance liée entre les parties, de dire si la situation est, ou non, constitutive d'un trouble manifestement illicite* », en d'autres termes de décider de l'application du droit (voire de le produire par interprétation). Symétriquement, s'est enrichie l'obligation des hébergeurs de lutter proactivement³²⁵ contre une certaine catégorie de contenus illicites. Cette catégorie posée par l'art. 6, I, 7 LCEN, initialement limitée à trois types de contenus en 2004 (apologies d'actes de terrorisme et de crime contre l'humanité, pédopornographie, incitation à la haine raciale), ne cessera de s'étoffer entre 2014 et 2016 pour y ajouter les contenus sexistes, homophobes et handiphobes, puis la provocation à la commission d'actes de terrorisme et enfin les contenus à caractère prostitutionnel ou représentant des violences sexistes³²⁶.

Le processus de responsabilisation des plateformes s'accélère dans la deuxième moitié de la décennie 2010 alors que les « plateformes » font leur entrée dans le droit positif de la consommation à travers la LRN d'octobre 2016. Spécialement obligées de livrer au consommateur une information « *loyale, claire et transparente* »³²⁷, ces plateformes sont identifiées selon deux genres d'activités³²⁸ : une qui les rapproche des ILT américains, à savoir

324BOSSAN Jérôme, « Le droit pénal confronté à la diversité des intermédiaires de l'internet », *Revue de science criminelle et de droit pénal comparé*, 2013, p. 295 et 302

325Cette lutte proactive implique le triple devoir pour l'hébergeur : (i) de mettre à disposition de l'utilisateur un dispositif de signalement des contenus listés par l'art. 6, I, 7 (TGI Paris, ord., 23 janv. 2013) ; (ii) d'informer « *promptement* » les autorités publiques compétentes d'un tel contenu dont l'hébergeur a eu connaissance ; (iii) de rendre consultables les moyens qu'il consacre à la lutte contre les activités illicites, généralement par leur inscription dans les conditions générales d'utilisation.

326Respectivement loi n° 2014-873 du 4 août 2014 pour l'égalité réelle entre les hommes et les femmes, loi n° 2014-1353 du 13 nov. 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, loi n° 2016-444 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées

327Code de la consommation, art. L111-7, II. Cette obligation implique de livrer au consommateur : (i) des conditions générales d'utilisation ; (ii) les modalités de référencement, de classement et de déréférencement ; (iii) l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération au profit de la plateforme ; (iv) l'identité de l'annonceur ; (v) lorsque le nombre de connexions mensuelles à une plateforme est supérieure à 5 millions de visiteurs unique, cette plateforme doit par ailleurs élaborer et rendre consultables des « *guides de bonne pratique en matière de clarté, de transparence et de loyauté* » et s'y tenir.

328Code de la consommation, art. L111-7, I

« le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers » (moteurs de recherche, comparateurs de prix, agrégateurs d'actualité...) ; ou une activité de « mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service » (marketplaces comme Amazon ou eBay, réseaux sociaux, Uber...). Dès 2019, l'utilité de ces nouvelles personnes juridiques dépasse le seul champ du droit de la consommation. Présentée à l'Assemblée Nationale en première lecture le 3 juillet de la même année, la proposition de loi visant à lutter contre la haine sur internet renvoie au Code de la consommation pour obliger les opérateurs de plateforme à retirer dans un délai de 24h (et non « promptement » contrairement aux hébergeurs non-opérateurs de plateforme) les contenus manifestement illicites qui leur sont signalés – incluant les contenus listés par l'art. 6, I, 7 LCEN et les discours haineux en ligne (dont sont exemptés les hébergeurs non-opérateurs de plateforme) – à défaut de quoi ces opérateurs encourraient une amende de 250 000€. Avant même l'entrée en vigueur de la loi, ce dispositif est toutefois censuré par le Conseil constitutionnel qui le déclare contraire à la liberté d'expression et de communication en 2020³²⁹.

Si le mouvement du droit positif semble suivre le même mouvement que l'évolution scientifique relatée, les autorités administratives de régulation se sont plus expressément appuyées sur les travaux des chercheurs. En 2017, le président de l'Arcep, Sébastien Soriano, relaie les conclusions rapportées dans ce II. pour disputer un « *Internet féodal* » dont les plateformes seraient les suzeraines³³⁰. Dans son rapport de 2014 sur « Le numérique et les droits fondamentaux », le Conseil d'État appelle de ses vœux un « *encadrement de l'utilisation des algorithmes* » en se référant à la gouvernementalité algorithmique de T. Berns et A. Rouvroy (contributrice au rapport)³³¹. La réflexion sur cet encadrement se poursuit avec la publication en décembre 2017 d'un rapport de la CNIL commandé par la LRN, proposant une régulation des algorithmes et de l'IA destinée à protéger les données personnelles, et s'inspirant elle aussi des analyses d'A. Rouvroy et de la *data-scientist* C. O'Neil théoriste des *Weapons of Math Destruction*³³². Conseillant le Premier Ministre depuis sa création par décret en 1997, le Conseil d'analyse économique adhère en 2015 aux explications susmentionnées (effet de réseau, RCA...) pour parvenir à la conclusion d'une domination économique par les plateformes, voire d'une dangerosité du cercle vicieux sus-décrit pour la concurrence européenne³³³.

329Aux motifs que ce mécanisme : (i) oblige à examiner tous les contenus signalés pour ne pas risquer la sanction pénale ; (ii) sachant que cette sanction peut intervenir au moindre défaut de retrait ; (iii) sans possibilité claire d'exonération pour l'opérateur ; (iv) alors que l'appréciation de l'illicéité même manifeste de certains de ces contenus appelle une « technicité juridique » ; (v) qui ne peut pas trouver de réponse satisfaisante dans un délai de 24h : CC, *Loi visant à lutter contre les contenus haineux sur internet*, 18 juin 2020, n° 2020-801 DC, §13-17

330SORIANO Sébastien, « Il est temps de renverser les seigneurs de l'Internet féodal », *Le Monde*, 5 juil. 2017 : « *Le modèle des plates-formes (Amazon, AppStore, etc.), qui a donné un accès inédit aux marchés à de nouveaux acteurs (développeurs, PME, particuliers), a aussi permis à certains de s'ériger en seigneurs imposant leurs lois (politiques de contenu, de référencement, de confidentialité, etc.), de façon unilatérale et parfois brutale.* »

331Conseil d'Etat, Rapport « Le numérique et les droits fondamentaux », 2014, p. 233s.

332CNIL, Rapport « Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle », 2017, p. 29-30

333COLIN Nicolas, LANDIER Augustin, MOHNEN Pierre et PERROT Anne, « Economie numérique », *Notes du Conseil d'Analyse économique*, 2015, n° 26, p. 1-12 ; BOURREAU Marc,

L'Union Européenne agit dans la même direction responsabilisante pour les plateformes. Dans la communication de la Commission européenne de 2017 « *Lutter contre le contenu illicite en ligne. Pour une responsabilité accrue des plateformes en ligne* »³³⁴, on retrouve les approches et arguments scientifiques qui, croisés, pointent vers les plateformes :

« Les plateformes en ligne par lesquelles la plupart des internautes passent pour accéder au contenu ont la lourde responsabilité, vis-à-vis de la société, de protéger les utilisateurs, et plus généralement le public, et d'empêcher les criminels et autres personnes impliqués dans des activités délictueuses d'exploiter leurs services [argument pragmatique, la plateforme est responsable du fait de son service]. Les espaces numériques ouverts qu'elles créent ne doivent pas être le terreau, par exemple, de la terreur, des discours de haine, de la pédophilie ou de la traite des êtres humains, ni devenir des zones échappant à l'État de droit [argument endogène des « espaces numériques », la plateforme est responsable du fait de son pouvoir numérique de création]. Il est clair que la diffusion de contenu illicite en ligne peut entamer la confiance du public dans l'environnement numérique, mais elle pourrait aussi menacer le développement économique futur de l'écosystème des plateformes et du marché unique numérique [argument informationnel-bien, les données sont des biens qui portent des enjeux économiques]. Du fait de la responsabilité découlant de leur rôle central dans la société, les plateformes numériques devraient résolument intensifier leurs actions pour traiter ce problème. (...) Étant donné la part de plus en plus importante qu'elles prennent dans la fourniture d'accès à l'information, les plateformes en ligne ont aussi un rôle clé à jouer pour établir cet équilibre [argument informationnel-communicationnel, la plateforme est responsable du fait de sa centralité dans la compréhension sociale humaine]. »

La même année, la CJUE régleme pour la première fois les critères algorithmiques utilisés (notamment par les services de police) pour analyser les données à des fins de lutte contre la criminalité grave et de protection de la sécurité publique. Les critères doivent être³³⁵ : (i) non-discriminatoires (selon le sexe, l'origine, la couleur de peau...) ; (ii) spécifiques et fiables (i.e. permettant « d'aboutir (...) à des résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité grave »). Outre des critères d'analyse, l'algorithme doit respecter deux autres conditions : (iii) les données traitées depuis la base de données doivent être « fiables, actuelles et limitées à la finalité de l'analyse » ; (iv) et une intervention humaine est obligatoire pour l'adoption de toute « mesure individuelle produisant des effets préjudiciables à l'égard des [personnes] concernées ».

En conclusion, dans la droite ligne des découvertes endogènes et de leur articulation avec les enseignements exogènes, le réseau internet n'est plus seulement régulé depuis des éléments qui lui sont extérieurs (machines ou acteurs humains) mais aussi, de façon grandissante, depuis des éléments qui lui sont internes (les contenus et algorithmes). L'identification de nouveaux concentrateurs de pouvoir dans les rapports de force sur internet a conduit à ce que **la**

PERROT Anne, « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du Conseil d'Analyse économique*, 2020, n° 60, p. 1-12

³³⁴ COM(2017)555, 28 sept. 2017

³³⁵ CJUE, Gde ch., Avis 1/15 du 26 juil. 2017 (sur le fichier PNR recueillant les données des passagers aériens)

connaissance ou le contrôle du contenu motivent désormais une régulation du réseau par responsabilisation des plateformes, ces dernières devenant ainsi l'un des principaux instruments contemporains de l'action juridique en ligne. Pourtant, que la régulation d'internet opère auprès des machines, des acteurs humains ou des contenus, elle nous semble négliger ou du moins taire une cause explicative de son inefficacité actuelle : la nature et l'effet prescriptifs des données en qualité, non d' « informations » humainement préhensibles, mais de données binaires exécutées par la machine.

Sous-Partie 2. La clandestinité (scientifico-étatique) des prescriptions numériques

On a constaté que la scission entre les vues exogènes et endogènes s'est progressivement atténuée depuis la fin des années 2000-début des années 2010, tant dans la réflexion scientifique que dans la régulation juridique. Par enrichissement mutuel des conclusions des chercheurs, le pouvoir en ligne exercé *au sein* d'internet est ramené principalement à deux composants informatiques du réseau maîtrisables par l'être humain. *Primo*, en tenant le code source pour enjeu de domination, les travaux endogènes les plus repris raccrochent le pouvoir en ligne au pouvoir d'encadrer les usages de l'utilisateur. *Secundo*, en tenant l'information en ligne pour enjeu d'exploitation, la majeure partie des travaux exogènes raccroche le pouvoir en ligne au pouvoir sur la signification humaine des données. Ces points de vue étudient donc : (i) le code informatique dans son seul versant « code source » (contraignant pour la machine et/ou l'utilisateur, ou servant une activité humaine) ; et (ii) la donnée dans son seul versant « informationnel » (appropriable tel un bien et/ou exprimable telle une communication).

De tels points de vue n'incluent dans l'analyse des rapports de force en ligne que les composants informatiques au moins partiellement comprises par l'être humain, au détriment des composantes exclusivement comprises par la machine que sont : (i) le code informatique *binaire* ; et (ii) la donnée elle aussi *binaire*. La compréhension de la machine conditionne son *utilisabilité*, *i.e.* les pouvoirs techniques octroyés à son utilisateur humain. Connaître les lois qui régissent cette compréhension binaire offrirait donc de savoir si et comment les caractéristiques internes à la machine déterminent ces pouvoirs techniques hérités d'internet.

Lorsqu'elle reçoit des données binaires, la machine ne les comprend pas autrement que comme des prescriptions, des ordres de mémoriser une règle exécutable ou d'exécuter cette règle. Un premier temps nécessitera de vérifier ce caractère prescriptif des données numériques (**Chapitre 1**). En comparant à cette occasion les prescriptions numériques et celles juridico-étatiques, on décèlera un pouvoir technique singulier que fournit l'utilisation d'internet à ses acteurs. Les lois internes à la machine, en déterminant l'utilisabilité humaine d'internet, dépassent l'intimité de la machine et inclinent les capacités et modalités de réalisation des rapports de force interhumains en ligne (**Chapitre 2**).

Chapitre 1. Le caractère prescriptif des données numériques

On recherchera les caractéristiques des données binaires en partant de la compréhension machinale qui en est faite. À plusieurs égards, et notamment en sciences de la Nature, le point de vue endogène a prouvé sa pertinence pour aborder l'influence de l'activité interne d'un objet sur des mouvements externes - tels des rapports de force interhumains (Section 1). En s'en

inspirant, on explorera l'activité interne à la machine numérique pour en extraire l'existence de « prescriptions numériques », n'existant comme telles qu'auprès de la compréhension machinale (Section 2).

Section 1. Le choix d'une méthodologie endogène pour l'étude des rapports de force en ligne

Si des zones d'ombres persistent dans les explications endogènes rapportées sur les rapports de force interhumains en ligne (Paragraphe 1), on exposera ici les raisons qui nous conduisent malgré tout à retenir une approche endogène de ces rapports (Paragraphe 2).

Paragraphe 1 – Des rapports de force inexpliqués par l'investigation endogène d'internet

Grand absent de l'étude endogène des rapports de force interhumains en ligne (A), le pouvoir de l'internaute ne trouve aujourd'hui sa place que dans des explications exogènes (B).

A) L'insuffisance des études endogènes pour la compréhension du pouvoir de l'internaute

Avant d'étudier la participation de l'internaute aux rapports de force en ligne, on délimitera le périmètre de cette figure pour savoir à quel acteur nous avons affaire concrètement. Dans les travaux scientifiques, l'internaute est surtout étudié dans sa situation (de consommateur, d'auteur, de profil surveillé, de communicant...), mais on en a trouvé peu de définitions explicites. On en relève deux distinctes selon les regards exogène/endogène.

Premièrement, en appliquant un regard exogène sur le réseau internet, la définition classiquement retenue est d'inspiration pragmatique. L'internaute est dans ce cas ramené à son activité d'« utilisation » du réseau internet. En ce sens, tel qu'il s'est popularisé en France depuis la fin des années 1990³³⁶, l'internaute équivaut à l'*internet user* anglais. Le dictionnaire Larousse confirme l'équivalence en caractérisant l'internaute comme l'« *utilisateur du réseau télématique Internet* ». Cette utilisation se manifeste à travers trois sortes d'actes : (i) l'« *accès au réseau Internet* » par « *un individu* » humain³³⁷ ; (ii) la diffusion d'informations *auto-identifiantes* signalant l'activité *personnelle* de l'internaute³³⁸ ; (iii) la publication de contenus, depuis l'essor au début des années 2000 du Web dit 2.0 ayant muni les utilisateurs d'aptitudes créatrices³³⁹ (blogs, forums, wikis, réseaux sociaux, avis consommateurs, plus récemment Discord...). Par conséquent, l'acte d'utilisation est à la fois (i) individuel (en accédant individuellement au réseau ou à un service internet, l'internaute fait acte de connexion pour son propre compte en tant qu'individu et non pour le compte d'un tiers comme une entreprise ou une association), (ii) personnel (les informations produites par l'internaute sont rapportables à son identité numérique personnelle, que cette identité numérique recoupe ou non son identité urbaine ou civile) et (iii) manuel (la publication de contenus par l'internaute requière une action physique de sa part, à la différence d'instructions logicielles qui automatisent une production de données).

336Par ex., WOLTON Dominique, *Internet et après ?*, Flammarion, 1999

337Définition donnée à l'« *internaute* » par l'Insee [en ligne]

338MOUNIER Pierre, *Les Maîtres du réseau*, préc., 2002, p. 146s. : « *puisque l'internaute est actif, puisqu'il choisit de rendre visite à tel ou tel site plutôt que tel autre, de regarder telle page plutôt que telle autre, puisque enfin il a la possibilité de transmettre des informations et d'échanger avec les gestionnaires d'un site ou d'un service, il délivre une somme infiniment plus importante d'informations sur lui-même que dans tout autre cas* »

339MALLET-BRICOUT Blandine, FAVARIO Thierry, *L'identité, un singulier au pluriel*, Dalloz, 2015, p. 79 : « *l'internaute, jusque-là utilisateur ou consommateur, va devenir éditeur de wikis, de forums de discussions, de sites de communautés, de blogs* »

Par comparaison, un programmeur libéral peut agir individuellement et personnellement en ligne, mais il opère en concevant un logiciel automatisant la production d'informations et non manuellement. Si le développeur n'est pas libéral, il accèdera au réseau et y produira des informations non à titre personnel mais pour le compte d'autrui, et son activité consiste toujours dans une production automatique d'informations. Ces trois critères *individuel (humain) / personnel / manuel* permettent ainsi de singulariser (en partant de son acte d'utilisation) l'internaute (synonyme d'utilisateur) parmi les autres acteurs qui pratiquent sur internet. On en conclut que, **selon un regard pragmatique** axé sur les activités en ligne, l'**internaute** peut être défini comme **la personne humaine qui fait une utilisation individuelle, personnelle et manuelle du réseau internet**. De nature pragmatique, cette définition évoluera au gré des pratiques³⁴⁰.

Deuxièmement, en appliquant un regard endogène sur le réseau internet, l'internaute n'est plus identifié d'après sa pratique, mais d'après les données comprises par la machine. Comment les données comprises par la machine permettent-elles à cette dernière de distinguer l'internaute du programmeur ? La distinction est claire : le programmeur stocke dans la mémoire de la machine des données d'instructions (instructions machine, instructions logicielles...) ; l'utilisateur stocke dans la mémoire de la machine des requêtes d'accès. Les données d'instruction sont des données *exécutables*, qui prévoient les opérations pouvant être effectuées par la machine ; les requêtes d'accès sont des données *à exécuter*, qui s'appuient sur des données d'instruction stockées pour ordonner les opérations que la machine doit appliquer à des données (message, clic droit ou clic gauche, capture d'écran...) dans un cas concret. Du point de vue de la compréhension machinale, le programmeur est donc le producteur de données qui stocke des données exécutables, tandis que l'utilisateur est le producteur de données qui stocke des données à exécuter. Le programmeur est donc synonyme de « créateur de données d'instruction », ou encore « créateur de logiciel » ; de son côté, l'utilisateur est synonyme d' « utilisateur de données d'instruction », ou encore d' « utilisateur d'un logiciel ».

Les données d'instruction sont *automatisables*, en ce sens qu'elles doivent être stockées une seule fois pour être réutilisables une infinité de fois sans devoir être produites à nouveau. Quant aux requêtes d'accès, elles sont soit *automatisées* (chaque requête est produite par un logiciel), soit *manuelles* (la production de chaque requête requiert une action physique). Que les requêtes d'accès soient automatisées ou manuelles, elles proviennent toujours d'un utilisateur qui se sert d'un logiciel – pour produire automatiquement ou manuellement ses requêtes. D'un point de vue endogène, **on définira donc le programmeur comme le producteur de données d'instruction** – donc fournissant à la machine ses capacités d'automatisation – et **l'internaute comme le producteur de requêtes d'accès produites manuellement ou automatiquement sur internet et depuis un terminal** – dans tous les cas sur la base de données d'instruction, donc d'un logiciel. C'est la définition qu'on retiendra tout au long de cette thèse, car elle offre une certaine stabilité théorique. Elle ne recoupe pas tout à fait la définition pragmatique : un programmeur qui travaille pour une entreprise aura systématiquement le statut de « programmeur » d'un point de vue pragmatique ; mais, d'un point de vue endogène, il n'agira en qualité de programmeur que

340Par ex. : le pullulement de profils « robots » automatisés sur les réseaux-sociaux ayant pour effet de brouiller la distinction entre « vrais » et « faux » internautes, le critère humain est-il destiné à demeurer ? La professionnalisation de l'internaute (rémunéré par des annonceurs dans le cas de l'« influenceur », embauché par des Etats dans le cas des *trolls farms*...) ayant pour effet de brouiller la distinction entre des internautes indépendants et des personnes agissant pour le compte d'autrui, le critère individuel est-il amené à être précisé ?

lorsqu'il stockera dans la machine des données d'instruction, et agira en tant qu'internaute chaque fois qu'il produira concrètement des requêtes d'accès, donc chaque fois qu'il ordonnera l'exécution de données par sa machine.

D'un côté, la position de l'internaute dans les rapports de force en ligne peut être sondée selon une rhétorique *complètement* endogène. En suivant cette rhétorique, les pouvoirs en ligne non seulement se déduisent de propriétés internes au réseau, mais par ailleurs s'exercent en son sein. On a pu relever deux principaux courants explicatifs aboutissant à cette « endogénisation » complète du pouvoir en ligne. D'abord, l'explication virtualiste de D. Post et D. Johnson exclut que le cyberspace puisse être régi depuis l'espace géographique, la liaison de ces deux espaces par les machines (*hardware*) n'étant pas de nature à déstabiliser la normativité issue de l'immatériel (*software*). Au lieu de se déplacer d'un lieu géographique à un autre comme le fait le citoyen, l'internaute se déplacerait d'un emplacement logiciel à un autre. Partant, le citoyen est régi par l'État (dont l'action s'applique à un territoire physique), tandis que l'internaute serait régi par les décisions du « sysop » (*system operator*, expression vieillie qu'on traduira actuellement par « administrateur de logiciel »)³⁴¹. Dans cette analogie entre le citoyen et l'internaute, le premier serait « moins » libre à l'égard de l'État que le serait le second à l'égard du sysop : ni physiquement ni matériellement contraint de demeurer dans un espace logiciel déterminé (site web, forum, appli...), l'internaute pourrait à tout moment quitter cet espace pour migrer vers un autre, s'évitant ainsi une « tyrannie »³⁴² des sysops. Tandis que la liberté endogène (ressortant des propriétés internes à la machine) du sysop s'exprimerait par le pouvoir de créer des espaces logiciels de contraintes, la liberté endogène de l'internaute consisterait à pouvoir choisir les contraintes auxquelles se soumettre. En sorte que, dans un cadre endogène, l'internaute (i) exercerait sa liberté en choisissant de se connecter ou non à un espace logiciel et (ii) s'assujettirait aux règles du sysop une fois cette liberté exercée. À l'appui de sa liberté tirée de la machine numérique, l'internaute ne pourrait donc s'autonomiser de l'action (ou de l'inaction) régulatrice d'un administrateur qu'en refusant d'accéder à l'espace logiciel de ce dernier³⁴³. Telle que résumée aux possibilités de rester sur un site web ou de migrer vers un autre, cette liberté endogène de l'internaute se heurte cependant à des phénomènes éprouvés en ligne tel le premier cas Jeuxvideo.com (JVC).

341JOHNSON David et POST David, « And How Shall the Net be Governed ? » in KAHIN Brian et KELLER James H. (dir.), *Coordinating the Internet*, MIT Press, 1997, p. 62s. : « tout opérateur de système [sysop, ici traduit par « administrateur de logiciel »] qui délivre un mot de passe impose au moins certaines exigences comme conditions de maintien de l'accès, notamment le paiement des factures à temps ou le fait de rester membre d'un groupe ayant droit à l'accès (par exemple, les étudiants d'une université). Les sysops disposent d'un outil extrêmement puissant pour faire respecter ces règles : le bannissement. »

342HARVEY David John, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age*, Bloomsbury/Hart Publishing, 2017, p. 107

343JOHNSON D. et POST D., « And How Shall the Net be Governed ? » in B. KAHIN et J. H. KELLER (dir.), *Coordinating the Internet*, préc., 1997 : lorsqu'un espace logiciel propose des contraintes non acceptées par l'internaute, ou lorsque cet espace plonge dans « l'anarchie » en abritant des contenus « nuisibles ou antisociaux » générés par les internautes, la seule option dont bénéficierait l'internaute au titre de sa liberté endogène serait l'évitement de cet espace.

Le premier cas Jeuxvideo.com (JVC)

Créé en 1997, ce forum devenu central dans la culture « alter » du Web s'est forgé une réputation sulfureuse en raison des comportements des internautes participants (propos haineux, harcèlement en meute, provocations diverses...), décourageant les entreprises à y déposer des annonces publicitaires pour ne pas y associer leur marque. Confrontée à la menace d'une perte de partenaires, la société actuellement détentrice du forum JVC, Webedia, décida en novembre 2017 d'y appliquer une censure algorithmique par mots-clés, en empêchant la publication de messages contenant certaines suites de caractères (par ex., « pute », « salope », féminazie » etc.). Les internautes contournent aisément l'algorithme en insérant dans les mots interdits des caractères indétectés par le logiciel (par ex., « pũte », « sālõpe » etc.), faisant alors abandonner cette méthode à Webedia.

Dans ce premier cas JVC, une mesure décidée par l'administrateur du logiciel pour régir les internautes bascule à cause des actions des internautes. Seulement, ces actions ne procèdent pas de la possibilité de se connecter à un espace logiciel, ni de celle s'y déconnecter, mais de la possibilité de contourner des règles logicielles. On en déduit que l'internaute : (i) exerce une liberté incluant d'autres possibilités d'action que le simple accès ou non-access à un site web ; et (ii) peut feinter les règles fixées par l'administrateur autrement que par le moyen de l'accès ou du non-access à ce site web. On en conclut que cette explication endogène de la liberté de l'internaute, résumée à la liberté de migrer d'un espace logiciel vers un autre, ne couvre ni toute la liberté ni tout le pouvoir des internautes dans leur rapport de force avec l'administrateur.

Ensuite, nous avons soulevé une deuxième explication complètement endogène : l'explication CodIL. Situait le *pouvoir endogène contraignant dans le seul code source et sa maîtrise*, elle ne permet pas davantage de comprendre comment dans le cas JVC les internautes *ont pu, sans manipuler le code source, contraindre* le contenu de l'espace logiciel dans un sens contraire à celui imposé par le rédacteur dudit code.

D'un autre côté, la position de l'internaute dans les rapports de force en ligne peut être sondée selon une rhétorique *partiellement* endogène. Les pouvoirs en ligne sont alors toujours inférés des propriétés internes au réseau, mais leur exercice est examiné à l'extérieur du réseau. J. Boyle et Y. Benkler partagent ici un point commun. Pour chacun de ces auteurs, le réseau numérique est un objet dont les caractéristiques techniques font naître un espace exclusivement composé d'informations, en tant que telles valorisables comme biens. Par la nature économique même de l'information, l'exploitation économique d'internet ne peut donc reposer que sur des informations-biens à la fois non rivales (la consommation d'une information ne diminue pas celle faite ou faisable par autrui) et non excluables (autrui ne peut être exclu d'une telle consommation). De cette exploitabilité collective germerait un espace informationnel par essence commun à ses membres. Cette explication nous semble avoir le mérite de proposer une cause endogène potentielle au phénomène observé dans le cas JVC d'une codétermination par les internautes du contenu d'un espace logiciel. En effet, des possibilités techniques fournies par le réseau pour son exploitation découlerait le pouvoir qu'a l'internaute de prendre part au contenu informationnel d'un tel espace logiciel. Mais si la nature du réseau internet est celle d'un espace informationnel commun exploitable par tous, comment expliquer que certaines informations présentes sur ce réseau (logiciels *open source* dont le code source est publiquement réutilisable, *wikis* dont

l'édition est ouverte aux internautes...) soient aisément exploitables par les internautes contrairement à d'autres informations (critères et résultats algorithmiques, données à l'accès chiffré...) ?

Aucun des trois questionnements soulignés (pour les explications virtualiste/CodIL/partiellement endogène) ne trouve de réponse endogène. Seules ont été proposées des explications exogènes.

B) Des explications exogènes au secours des insuffisances endogènes

En premier lieu, bien que la liberté de migration avancée par l'explication virtualiste ne permette pas de cerner les libertés et pouvoirs exercés par l'internaute dans le cas JVC, D. Johnson et D. Post n'ignorent pas lesdits pouvoirs et libertés. Ces derniers sont toutefois rapportés à des mécanismes communicationnels (humains) et non plus endogènes (machinaux). Les deux auteurs invoquent l'exemple des adresses mail fournies dans les années 1990 par la société AOL et spécifiées par le label <.aol> inséré dans l'adresse. Auprès des internautes de la première heure, ce label devient le marqueur social des nouveaux internautes « grand public », puis l'objet de moqueries de la part des vieilles générations d'internautes à l'encontre des nouvelles. Cette discrimination « *domainiste* »³⁴⁴ s'appuyant sur des informations attachées à un compte en ligne plutôt que sur des éléments révélateurs de la *personnalité* (couleur de peau, sexe, identité civile...), le droit à ne pas être discriminé tel que garanti juridiquement ne s'y appliquerait pas pertinemment. Les expressions en ligne façonneraient des constructions communicationnelles axées sur des informations plutôt que sur la personne qui en est l'auteur ou la victime. Dans ce cadre communicationnel, la « personne » ne saurait servir de point de départ adapté à la régulation d'internet. Pour enrayer certaines constructions communicationnelles (comme le domainisme discriminant ou le chaos expressif de type JVC), seule serait donc efficace une action régulatrice ciblant les communications en ligne. Or, du fait de la décentralisation architecturale du réseau internet vers les terminaux et de la domination logicielle des sysops, une telle action régulatrice ne pourrait provenir que de deux acteurs : les internautes (*via* la production de communications depuis leur terminal) ; et les administrateurs de logiciel (*via* la réglementation des capacités d'utilisation de leur logiciel). L'autorégulation s'imposerait ainsi *de facto* d'après ces auteurs, qui préconisent une condamnation communicationnelle des comportements nuisibles, par ex. en inscrivant ces comportements dans la Nétiquette (charte non-officielle documentée par la RFC 1855 de 1995, ne faisant plus vraiment autorité en 2021, émanant d'un processus délibératif informel destiné à recenser et à inhiber les conduites néfastes parmi les communautés en ligne).

Les espaces logiciels seraient dès lors « *collectivement contrôlés* »³⁴⁵ par les internautes et administrateurs qui, ensemble, élaborent les « *règles* » composant l'autarcie normative du cyberspace. De nature communicationnelle, le pouvoir des internautes dans l'élaboration de ces règles serait donc d'effet purement incitatif (p. ex. à travers la Nétiquette). En appliquant cette hypothèse au cas JVC : les internautes peuvent inciter Webedia à retirer son algorithme de modération, ou décourager d'autres internautes à visiter le forum ; mais seul Webedia peut

344JOHNSON David et POST et David, « Law and Borders... », préc., *Stanford Law Review*, 1996, p. 1401

345 *Ibid.*, p. 1393 : « Si les sysops [administrateurs de logiciels] et les utilisateurs qui habitent et contrôlent collectivement une zone particulière du Net veulent établir des règles spéciales pour y gouverner leur conduite, et si cette règle n'empiète pas fondamentalement sur les intérêts vitaux des autres qui ne visitent jamais ce nouvel espace, alors la loi des souverains dans le monde physique devrait s'en remettre à cette nouvelle forme de gouvernement autonome. »

contraindre les facultés d'utilisation de JVC, ou empêcher des internautes d'accéder au forum. Le cas JVC trouve par-là explication grâce à une argumentation exogène-communicationnelle.

En deuxième lieu, l'explication CodIL se reporte également sur des causes exogènes pour comprendre la position de pouvoir de l'internaute. Sur ce point, a déjà été précisée la pensée de L. Lessig selon laquelle les rapports de force en ligne sont émis depuis une source endogène (maîtrise du code) et des sources exogènes (normes sociales, lois du marché, règles de droit). Tout au long de son ouvrage *Code*, L. Lessig situe le pouvoir des internautes dans les normes sociales qu'ils édictent en ligne³⁴⁶. Dans le même sens, on a largement illustré que, parmi les combinaisons de l'explication CodIL avec les enseignements exogènes, la combinaison avec l'approche communicationnelle est quasiment la seule à démontrer l'existence d'un pouvoir en ligne possédé et cultivé par l'internaute (pouvoir de nature expressive suivant cette combinaison). Ni L. Lessig, ni aucune de ces combinaisons ne déclare une nature endogène au pouvoir de l'internaute.

En troisième lieu, la position partiellement endogène cite à son tour des raisons exogènes, cette fois économiques et non plus communicationnelles, pour expliquer l'exploitabilité différenciée des informations en ligne en dépit de la propriété informationnellement commune d'internet. Pour Y. Benkler et J. Boyle, le cyberspace étant structuré par des informations par ailleurs assorties de la qualité de « biens », le pouvoir sur ce cyberspace s'exercerait par le biais des droits réels détenus sur ces biens.

Y. Benkler, d'abord, considère ces droits réels aussi factuels que l'est le caractère commun de l'information en réseau : le réseau étant *de facto* constitué de communs informationnels, chacun pourrait de fait exercer sur une information-bien en réseau les droits réels qui s'attachent à un bien commun (libre accessibilité et exploitabilité d'un bien transformé par l'action collective). En d'autres termes, quels que soient les droits *juridiquement* reconnus sur une information en ligne, cette information préserverait *factuellement* sa qualité de bien commun avec les droits réels qui en découlent.

Les droits réels détenus de fait par l'internaute sur l'information ne diffèrent donc pas de ceux détenus par les autres acteurs du réseau. Néanmoins, ce nivellement théorique du pouvoir sur l'information dissone fortement avec la variation des pouvoirs de l'internaute selon que l'information est publique/ouverte (pouvoir de contribution au *design* d'un logiciel dans l'hypothèse d'une conception participative, pouvoir d'édition d'un *wiki*, pouvoir de réutilisation de contenus libres de droit...) OU privatisée/fermée (impossibilité de concourir aux règles algorithmiques opaques d'un logiciel propriétaire³⁴⁷, impossibilité d'exploiter le nom de domaine d'une marque³⁴⁸, impossibilité d'accéder à une œuvre protégée par

³⁴⁶L. Lessig étudie notamment cette normativité sociale à travers les forums et *newsgroups* de Usenet, le jeu vidéo *Second Life* etc.

³⁴⁷ Le logiciel est appropriable au titre du droit d'auteur (art. L. 122-6 Code de la propriété intellectuelle en France depuis la loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle). Depuis 1986, l'Office Européen des Brevets admet la brevetabilité, non d'un algorithme lui-même, mais du support physique dans lequel il est intégré un algorithme et à l'originalité duquel support il contribue (OEB CRT, ch. des recours techniques, aff. *Vicom*, 15 juil. 1986, n° T-208/84:JO OEB 1/1987).

³⁴⁸ Par ex., en guise de cadeau d'anniversaire pour sa mère prénommée « Milka », une personne ne peut acquérir le nom de domaine <milka.fr> aux fins de l'exploiter pour une activité commerciale de couture sans, par-là, porter « préjudice » à la marque de chocolat Milka, bien que les deux sociétés ne

DRM...). Les critiques les plus couramment dirigées contre cette théorie benklerienne lui reprochent ainsi son imperméabilité à l'égard d'une telle variation des pouvoirs en ligne impulsée par l'appropriation juridique de certaines informations³⁴⁹.

Quant à J. Boyle, il s'épargne cette opposition en reconnaissant au contraire le droit positif comme un paramètre déterminant de la variation des pouvoirs de l'internaute : si l'information en ligne est un commun *de facto*, les droits réels qui s'y appliquent résultent eux de leur consécration *de jure*. En 2003³⁵⁰, notant la consécration grandissante de droits de réels sur les données (DRM, prolongement du droit d'auteur de 28 à 70 ans après le décès de l'auteur aux États-Unis, brevetabilité américaine des logiciels, condamnation juridictionnelle des P2P sur le fondement du DMCA, droit européen de producteur de bases de données ³⁵¹ ...), J. Boyle en conclut que l'internaute est juridiquement dépossédé de son pouvoir technique de participer à la construction collective d'un bien informationnel commun par essence ³⁵². Les règles de droit interposeraient des possibilités d'exclusion et interdictions d'accès là où l'information en ligne est en principe non-excluable. L'auteur y voit un second mouvement d'*enclosures* succédant à celui du XVI^e siècle :

se concurrencent pas sur le même segment de marché, dès lors que « à la différence du nom patronymique, le prénom ne confère aucun droit privatif à son titulaire sauf (...) à démontrer qu'elle a acquis une certaine célébrité sous ce prénom » (CA Versailles, 12^e ch., 27 avr. 2006). Le nom de domaine <milka.fr> doit alors être transféré sans frais à la société Kraft Foods détentrice de la marque Milka.

349BROCA Sébastien, Entrée « Benkler (Yochai) » in CORNU M., ORSI F., ROCHFELD J. (dir.), *Dictionnaire des biens communs*, préc., PUF, 2017, p. 81 : « les travaux [de Y. Benkler] négligent certaines questions dont le renouveau d'une économie politique marxiste appliquée à Internet (...) a cherché à montrer la saillance [avec les concepts de capitalisme cognitif, libéralisme informationnel, digital labor...]. (...) Benkler livre ainsi peu d'éléments d'analyse et de critique sur les multiples formes de récupération marchande des communs numériques et sur l'exploitation de travail gratuit (digital labor) à laquelle ils donnent souvent lieu. Il présente la coexistence entre la production de communs et le développement du capitalisme numérique incarné par les grandes entreprises de la Silicon Valley (...) comme non-problématique et mutuellement bénéfique (...). Dans certaines interventions plus récentes, il s'est toutefois montré plus critique envers les principaux représentants (Uber, Airbnb) de "l'économie du partage" (Benkler, 2015). »

350BOYLE James, « The Second Enclosure Movement and the Construction of the Public Domain », *Law and Contemporary Problems*, vol. 66, 2003, p. 34-74

³⁵¹ Issu de la directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données, ce droit « *sui generis* » consiste pour le producteur d'une base de données à exercer un droit d'auteur sur sa base et à « *interdire l'extraction et/ou la réutilisation non autorisées de la totalité ou d'une partie substantielle du contenu* » de la base (art. 7)

³⁵² Sur le pouvoir contributif de l'internaute à l'égard de l'information en ligne comme bien commun : BOYLE James, *The Public Domain. Enclosing the Commons of the Mind*, Yale University Press, 2008, p. 179s.

« Le premier mouvement des enclosures est le symbole de la modernité capitaliste émergente, du remplacement de l'ancien par le nouveau, du renversement des modes de vie traditionnels par le "progrès". Le second mouvement (...) apparaît au contraire (...) comme l'ultime soubresaut de l'ancien monde pré-Internet, le champ du cygne des "vieilles" industries culturelles, la résistance désespérée de la société industrielle face à une société de l'information en train d'éclore. (...) Pour le dire en termes marxistes : dans le premier cas, l'essor de la propriété privée allait dans le sens du développement des forces productives ; dans le second, elle apparaît au contraire comme une entrave à celles-ci ».

Tout en maintenant que les propriétés techniques du réseau font de l'information un bien commun instaurateur d'un espace économique collectivement exploitable, J. Boyle parvient ainsi à expliquer la fluctuation du pouvoir des internautes selon les droits réels juridiquement exercés en ligne. Aussi divergentes soient leurs analyses, Y. Benkler comme J. Boyle évaluent la place de l'internaute dans les rapports de force en ligne à partir d'une cause exogène au réseau : les droits réels exercés sur l'information (factuels pour Y. Benkler, juridiques pour J. Boyle).

On note alors que les études complètement ou partiellement endogènes n'apportent d'explication au pouvoir de l'internaute qu'à l'appui de causes exogènes. Pour le dire autrement, **le pouvoir de l'internaute** – tel que celui observé dans le cas JVC contre un logiciel propriétaire (algorithme de modération d'un forum administré par une société commerciale) – **reste un mystère endogène**. Avant de proposer une clarification de cette énigme, on s'inspirera des apports des sciences de la Nature qui nous offrent de répondre à deux questions : en quoi l'examen endogène d'un objet nous apparaît-il pertinent pour comprendre des rapports de force extérieurs à cet objet ? Et quelle méthodologie endogène appliquer au réseau internet pour examiner les rapports de force en ligne ?

Paragraphe 2 – La pertinence du regard interne pour la compréhension de mouvements externes

En mettant la lumière sur l'existence de lois internes à l'objet physique distinctes des lois le régissant extérieurement (A), les découvertes des sciences de la Nature au XIX^e siècle ont fait voir l'influence de ces lois internes auprès de l'environnement extérieur à l'objet (B).

A) Lois internes et lois externes d'un objet

Jusqu'au XIX^e siècle, les physiciens s'accordaient sur l'hypothèse que les lois de la physique (lois de la gravité, de conservation, de la thermodynamique...) s'appliquaient pareillement à un objet, tant dans sa composition (monde microscopique de l'infiniment petit) que dans son appartenance au monde extérieur (monde macroscopique de l'humainement visible, et univers de l'infiniment grand). À titre d'illustration, d'après les lois de la thermodynamique, un corps est en mouvement sous l'effet de l'énergie (notamment dégagée par la chaleur) qu'il reçoit³⁵³. Or, en 1828, le botaniste Robert

³⁵³Sur une vulgarisation très claire des lois acquises en physique classique (thermodynamique, champs de force, électromagnétisme...) et de leur dépassement par la physique quantique, v.

Brown observe au microscope que, déposées dans un volume d'eau, des graines pivotent et se déplacent bien qu'elles soient mortes depuis des décennies et qu'elles aient perdu toute faculté de fécondation (pollen). Le constat d'un mouvement (dit « brownien ») des corps est le même quand R. Brown dispose des bris de verre sur l'eau³⁵⁴. À l'inverse des lois connues de la thermodynamique, la matière de très petite taille se meut sans se nourrir d'énergie ou en être nourrie.

Les atomistes de la fin du XIX^e siècle y voient la possible preuve que toute matière est composée d'atomes, de minuscules particules dont les actions sont ignorées du monde extérieur et de ses lois. Cette preuve d'une réalité interne à la matière sera apportée par la cohérence mathématique. D'après la théorie atomiste, l'atome serait le centre de production des charges électriques. La matière induirait sa propre énergie depuis sa composition, ce qui expliquerait l'indépendance de la mobilité des graines vis-à-vis de la variation des paramètres extérieurs (excepté la chaleur, comme la lumière, le champ magnétique...) ³⁵⁵.

Précisément, cette énergie électrique est libérée sous forme d'ondes électromagnétiques, de « rayonnements » émis chaque fois que l'atome change de vitesse. Afin de mesurer l'activité électrique renfermée par ces ondes, le physicien Hendrik Lorentz calcule l'énergie ainsi libérée dans l'interstice qui sépare deux longueurs d'onde (*i.e.* l'espace entre deux maximas d'une onde). Grâce au nombre de changements de vitesse observés entre deux longueurs d'onde, H. Lorentz évalue à 77.10^{22} le nombre d'atomes compris dans cet interstice (le nombre sera toutefois corrigé à 66.10^{22} par Charles Féry³⁵⁶). Parmi ces rayonnements électromagnétiques issus des atomes, le chimiste-physicien Ernest Rutherford s'intéresse aux rayons X qui émanent d'un corps radioactif. L'action atomique n'est plus ici étudiée à partir de changements de vitesse, mais à partir des projectiles de rayons X diffusés par ce corps. Dans leur propagation, ces projectiles se heurtent à l'hélium généré par la diminution naturelle de la radioactivité du corps avec le temps. L'hélium ainsi dégagé est lui aussi fractionnable dans sa masse, par exemple en portions d'1 g si l'on souhaite calculer le nombre d'atomes inclus dans 1 g d'hélium. Il est en effet possible de connaître ce nombre en connaissant (i) la masse d'hélium échantillonnée et (ii) la quantité de projectiles émise en une seconde, en ce qu'ils traduisent l'action atomique des rayons X. En s'appuyant sur cette cadence des projectiles, E. Rutherford évalue ainsi à 71.10^{22} le nombre d'atomes contenus dans 1 g d'hélium au contact de rayons X, soit un résultat extrêmement proche de celui obtenu par H. Lorentz (même corrigé). Entre 1907 et 1909, réalisant une expérience théorisée par Albert Einstein, Jean Perrin tente à son tour de calculer le nombre d'atomes contenu dans 1 g d'eau. Pour ce faire, il répète l'expérience de R. Brown en déposant des grains de mastic dans un volume d'eau et comptabilise, à partir du déplacement des grains, le nombre de fois que les particules d'eau percutent les grains sur une fraction d'une seconde. Tout comme les projectiles traduisent l'action atomique des rayons X, ces percussions traduisent l'action atomique de l'eau, *i.e.* l'énergie électrique autoproduite par l'eau. De la même façon, il est donc possible d'en déduire le nombre d'atomes inclus dans l'eau en connaissant (i) la masse d'eau échantillonnée et (ii) la quantité de percussions occasionnées en

BERRAH Nora, HUMPHREY Marc, PANCELLA Paul, VAUDREY Catherine, *Physique quantique. Le guide de référence*, Les éditions Trédaniel, 2019

354 ROLLET Vincent, *La physique quantique (enfin) expliquée simplement*, Institut Pandore, 2014, p. 9

355 C'est le physicien Léon George Gouy qui démontrera cette indépendance en 1888

356 PERRIN Jean, « Mouvement brownien et molécules », *Journal de physique théorique et appliquée*, 1910, p. 38 [en ligne sur HAL]

une seconde. J. Perrin obtient un résultat parfaitement identique à celui d'E. Rutherford en dénombrant 71.10^{22} atomes dans 1g d'eau.

Quel que soit le moyen de démonstration emprunté (par les changements de vitesse, la cadence des projectiles, la fréquence des percussions...), quel que soit le phénomène étudié (ondes électromagnétiques, hélium au contact de rayons X, mouvement brownien...), les expériences convergent chaque fois vers le même nombre alors que, « *pour chacun de [ces phénomènes] (...) on pourrait attendre n'importe quel jeu de valeurs comprises entre zéro et l'infini* »³⁵⁷. La valeur mathématique de l'action atomique étant la même pour tous ces phénomènes, est ainsi démontré que ces derniers sont transcendés par une action atomique universelle malgré leur disparité dans le monde de la physique classique (macroscopique et univers). Huit décennies après la découverte du mouvement brownien, sa cause atomique est par-là prouvée en même temps que l'existence de l'atome.

Ceci établi, les sciences de la Nature peuvent inspecter cet atome, constater les lois auxquelles il obéit. Et ces lois s'avèrent bien éloignées des lois de la physique classique. Le mouvement brownien, a-t-on pu voir, a déjà révélé l'inadaptation des lois de la thermodynamique au monde microscopique. N'y est pas davantage applicable la scission connue de la physique classique entre l'onde (immatérielle) et la particule (matérielle).

Pour en arriver à cette conclusion, la lumière fut le terrain privilégié d'expérimentation. Depuis les travaux de Thomas Young 1801, il est acquis que la lumière agit comme une onde. Pour son expérience, T. Young projette un éclairage sur une plaque perforée par deux fentes ; les faisceaux de lumière traversent les fentes pour atteindre un écran situé derrière la plaque ; mais l'écran, au lieu de faire apparaître deux traits de lumière correspondant à l'emplacement des fentes, laisse voir une pluralité de bandes sur toute la surface de l'écran. En se *diffractant* ainsi, la lumière exerce une capacité dont sont dépourvues les particules et qui est spécifique aux ondes. L'action ondulatoire de la lumière est alors prouvée en physique classique. Étudiant la lumière dans le monde microscopique, A. Einstein note cependant un tout autre résultat à l'aune des découvertes électriques et atomiques récentes : en 1888, H. Hertz remarque qu'un métal, une fois éclairé, produit de l'énergie électrique par la réception de cette lumière ; Philipp Lenard y ajoute toutefois qu'une lumière de faible intensité (faible longueur d'onde ou faible fréquence de l'onde) ne permet pas au métal de produire une telle énergie. Cherchant à comprendre ce rapport intensité de la lumière/énergie produite par le métal, A. Einstein propose l'explication suivante : les électrons ne peuvent se détacher du métal, et donc dégager de l'électricité, que si l'énergie transmise par la lumière est supérieure à l'énergie qui lie les électrons au métal³⁵⁸. Cependant, une telle explication contredit les lois de la physique classique selon lesquelles une onde électromagnétique (comme la lumière) ne peut transmettre de l'énergie électrique. Seule une particule détient cette capacité. Indéniablement, la lumière agit comme une onde. Mais elle agirait aussi comme une particule. Dans le monde microscopique, la lumière n'est ni exclusivement onde, ni exclusivement matière, mais onde et matière à la fois ; elle est « *photon* », selon l'appellation du chimiste Gilbert Lewis. La validité de cette dualité onde-particule pour tout objet en mouvement (atome, molécule, table, hérisson...) sera mathématiquement proposée par le physicien de Broglie au début du XXe siècle, avant d'être empiriquement

³⁵⁷*Ibid.*, p. 39

³⁵⁸ROLLET Vincent, *La physique quantique*, préc., 2014, p. 37

confirmée en 1927 par les physiciens Clinton Davisson et Lester Germer³⁵⁹. Là où l'onde et la matière répondent chacune à des lois distinctes en physique classique (scission onde-particule), elles sont indivisiblement soumises aux mêmes lois en physique quantique (dualité onde-particule).

Outre la thermodynamique et la relation onde-particule, les lois quantiques contredisent encore les lois classiques sur la prévisibilité des mouvements. En physique classique, la trajectoire d'une balle de baseball par exemple peut être prédite si toutes les données requises pour ce calcul sont connues (vitesse de la balle, masses de la batte et de la balle, prise de la batte, angle de frappe...). *A contrario*, en physique quantique, il est par exemple impossible de prévoir avec précision les étapes d'évolution d'un corps radioactif. En effet, on a vu que, le temps passant, un tel corps réduit naturellement sa radioactivité : les noyaux de ses atomes radioactifs subissent des modifications successives (« transmutations ») qui ont pour effet de « désintégrer » l'atome, d'en changer l'élément radioactif (par ex. du plutonium) en un élément stable (du plomb). Tout au long de cette chaîne radioactive – au cours de laquelle la désintégration du plutonium passera par plusieurs étapes comme l'uranium, le radium, le polonium jusqu'à devenir du plomb –, la désintégration de l'atome est chronologiquement imprévisible. *« Alors qu'en physique classique, le système étudié peut se trouver dans un état indépendant de tout observateur et être mesuré sans perturbation, en physique quantique une mesure est un processus plus complexe, dans lequel l'état de l'objet mesuré est en général modifié »*³⁶⁰. La composition microscopique de la balle de baseball (aux actions atomiques imprévisibles) ne répond pas aux mêmes règles que la réalité macroscopique de la même balle (aux mouvements prévisibles).

À travers ces trois illustrations (thermodynamique, onde-particule, certitude classique), on a voulu rappeler la preuve apportée par les sciences de la Nature que toute matière possède une activité interne différemment régie de son activité externe. De la même façon que des lois quantiques régissent l'activité atomique, on posera la **première hypothèse que des lois numériques** (binaires) **régissent l'activité des données binaires** – hypothèse qu'on expérimentera plus loin [v. *infra*]. Par ces illustrations, on a aussi voulu souligner que la seule voie de démonstration ayant permis d'identifier l'autonomie atomique interne à tout objet fut le regard endogène porté sur cet objet. Or, cette conception endogène ne s'arrête pas à observer l'existence d'une telle autonomie : elle rend analysables les influences déployées par ces lois internes sur l'activité extérieure de l'objet.

B) Lois internes et environnement externe de l'objet

Aussi autonomes soient-elle des lois externes, les lois internes à l'objet étendent pourtant leur action aux mouvements extérieurs. Le corps radioactif nous en a fourni un exemple typique. Les désintégrations de l'atome jusqu'à sa stabilisation modifient l'environnement du corps : l'hélium (radioactivité alpha) ou les positons (radioactivité bêta et gamma) provenant de désintégrations internes se diffusent bien à l'extérieur du corps ; de même, après transmutation de l'atome radioactif en atome de plomb, les rayons émis par l'activité interne à ce corps deviennent inoffensifs pour l'être humain qui lui est extérieur. Dans ce dernier cas, l'action

359BERRAH N., HUMPHREY M., PANCELLA P., VAUDREY C., *Physique quantique. Le guide de référence*, « Partie 3. Mécanique quantique, 8. Les ondes de matière », préc., 2019

360HAROCHE Serge, « Mesures quantiques non destructives », Première leçon du 21 janv. 2008, Cours 2007-2008 au Collège de France [en ligne sur le site du Collège de France]

atomique altère l'utilisabilité humaine de l'objet (roche radioactive par ex.) en faisant évoluer sa dangerosité.

La dangerosité n'est qu'un lien parmi d'autres entre l'activité interne d'un objet et son utilisabilité externe. La praticité, i.e. l'emploi optimal d'un objet, est un autre de ces liens qu'on peut illustrer par les innovations fondées sur la physique quantique. Certaines des innovations technologiques récentes se sont en effet reposées sur une loi propre au monde microscopique : la superposition quantique. Suivant ce principe, une particule microscopique (atome, molécule, électron...) peut se trouver dans deux états contraires en même temps *jusqu'à ce qu'elle soit mesurée*. Pour s'en faire une idée concrète, V. Rollet utilise la métaphore du billet de loterie : « *Avant le tirage du numéro gagnant, le billet n'est ni gagnant ni perdant, il a une certaine probabilité d'être gagnant et une certaine probabilité d'être perdant, il est dans la superposition des deux états gagnant et perdant. Après le tirage, l'état du billet « s'effondre » : il est soit gagnant, soit perdant, il n'y a plus d'incertitude.* ».³⁶¹ Le tirage symbolise ici la mesure humaine d'un état quantique. Tout comme le tirage « arrête » l'état gagnant/perdant, la mesure « arrête » un état quantique³⁶². Pour autant, la réalité microscopique ne fixe pas un état déterminable : « *avant toute mesure, un électron autour d'un noyau ne se situe pas à un endroit précis : sa position n'obéit qu'à des probabilités, et on ne peut pas vraiment dire où il est. Après la mesure, l'électron est fixé en un point, là aussi, l'incertitude disparaît.* »³⁶³. Toute matière jaillit d'une superposition d'états qui, paradoxalement, sont contradictoires dans le monde macroscopique où cette même matière prend place. Le physicien Erwin Schrödinger métaphorisa une superposition des états mort/vivant, et son homologue Hugh Everett, une superposition d'univers parallèles créés lors d'une mesure de l'activité quantique.

Plus récemment, le principe de superposition quantique a fait l'objet d'une industrialisation avec la réalisation de l'ordinateur (ou calculateur) quantique. En 2009, pour le compte de l'Université de Yale, une équipe de physiciens publie ses travaux synthétisant son invention du premier ordinateur quantique doté de qubits³⁶⁴. À la différence du bit numérique qui n'offre à l'ordinateur qu'une option binaire (0 pour non/faux/négatif, 1 pour oui/vrai/positif), le qubit ou « bit quantique » exploite la superposition des états physiques pour fournir à la machine une infinité théorique de choix (le 0 et le 1 se superposant au lieu de se succéder).³⁶⁵ Cela signifie aussi qu'une IA

361ROLLET V., *La physique quantique*, préc., 2014, p. 98

362La structure fondamentalement probabiliste de la mécanique quantique oblige alors à lui appliquer des outils de mesure spécifique. L'état quantique à un instant T, encore appelé « l'observable », est ainsi évalué et décrit par un « opérateur » (par exemple hermitien) donnant notamment la possibilité de réaliser une mesure généralisée des différents états empiriquement traversés par une structure quantique (POVM) voire de probabiliser les états hypothétiquement traversés par cette structure en projetant un état après sa mesure (mesure projective de von Neumann). À ce propos, v. notam. ANTOINE Charles, *Introduction à la physique quantique*, Dunod, 2020, p. 69-104

363ROLLET V., *La physique quantique*, préc., p. 98

364DICARLO Leonardo, CHOW Jerry M., GAMBETTA Jay M., BISHOP Lev S., JOHNSON Blake, SCHUSTER David, MAJER Johannes, BLAIS Alexandre, FRUNZIO Luigi, GIRVIN Steven et SCHOELKOPF Robert, « Demonstration of two-qubit algorithms with a superconducting quantum processor » [en ligne], *Nature*, n° 460, 2009, p. 240-244

365Sur la manière dont les qubits peuvent être couplés ensemble et utilisés pour le traitement de l'information, v. notam. le cours 2010-2011, « Synthèse, contrôle et protection d'états quantiques » donné par Serge Haroche au Collège de France sur l'année 2010-2011, et en particulier les troisième et quatrième leçons des 24 et 31 janv. 2011, respectivement « Les qubits supraconducteurs » et « L'information quantique avec des qubits de phase » [en ligne sur le site du Collège de France]

dont les actions dépendent de qubits serait en principe délivrée de son cadre binaire actuel qui l'oblige à réagir par signaux positifs ou négatifs à une kyrielle d'opérations. En 2019, un partenariat liant Google AI et la NASA débouche sur la première résolution par ordinateur quantique d'un problème irrésolvable par ordinateur binaire. La différence de composition et d'activité atomiques entre une IA « quantique » et une IA « binaire » emporte une différence quant à leurs utilisabilités afférentes. Les possibilités techniques mise à la disposition humaine (résolution d'un problème en l'espèce) ne sont pas les mêmes d'une IA à l'autre.

Mises à part des fins de praticité, la composition atomique de l'objet peut encore servir des fins de sécurité à l'aide d'un autre principe quantique : l'effet de Zénon. Corolaire de la superposition quantique, l'effet de Zénon implique que la mesure d'un objet fige son état ; cet objet ne peut pas transmuter ni se désintégrer lors de la mesure. Donnant la faculté de bloquer l'évolution d'un système quantique, cet effet est exploité en 2017 par un groupe de physiciens chinois afin de réaliser la première « communication quantique contrefactuelle », *i.e.* la première transmission d'un message d'un endroit à un autre *via* un canal quantique sans le moindre déplacement de particules³⁶⁶. Lorsque le canal perçoit des particules, il rejette la transmission et renouvelle son système atomique. Il est « bloqué » dans son évolution, s'auto-détruit pour se restructurer dès qu'il perçoit une variation particulière. Impénétrable par une source non-désirée, ce canal offre de sérieux moyens de sécurisation d'un réseau. Est alors concevable l'essor d'un réseau quantique dont les échanges seraient soumis à de nouvelles lois internes, divergeant de celles valables pour les communications binaires, et qui ouvrent des possibilités d'utilisation encore inconnues, modifient l'utilisabilité de l'objet « réseau ».

Comme on a pu le voir avec la radioactivité puis la superposition quantique et l'effet de Zénon, les lois qui régissent l'intérieur d'un objet transforment son rapport à l'environnement extérieur (dangerosité, praticité, sécurité... de l'objet pour l'être humain) et, par-là, son utilisabilité humaine. Bien que ces lois ne déterminent pas l'utilisation effectivement faite de l'objet, leur compréhension ouvre la maîtrise de certains phénomènes externes. Parmi les phénomènes externes ainsi influencés par l'activité atomique interne de l'objet, on s'intéressera spécifiquement aux rapports de force interhumains. On rappelle notre définition attribuée en Introduction au *rapport de force interhumain* comme étant (i) *un type de relation interindividuelle ou de groupe par laquelle* (ii) *des êtres humains* (iii) *imposent concrètement* (iv) *leurs actes et/ou décisions à d'autres êtres humains*.

En appliquant cette définition au cas de l'IA par exemple (fictif) : sur un marché économique (i) où se nouent des relations concurrentielles, (ii) les entreprises équipées d'une IA quantique pourraient atteindre une productivité telle (iii) qu'une distorsion de concurrence se creuserait à cause (iv) de l'utilisation par ces entreprises d'une IA quantique dont ne peuvent se munir d'autres entreprises partageant un même segment de marché, réduites à l'utilisation d'une IA binaire et victimes de pertes d'argent du fait de cette distorsion. L'évolution de la composition interne de l'objet « IA » (quantique/binaire) entraîne une évolution des rapports de

366YUAN Cao, YU-HUAI Li, ZHU Cao, JUAN Yin, YU-AO Chen, HUA-LEI Yin, TENG-YUN Chen, XIONGFENG Ma, CHENG-ZHI Peng, JIAN-WEI et Pan, « Direct counterfactual communication via quantum Zeno effect » [en ligne], *PNAS*, vol. 114, 2017, p. 4920-4924. Pour voir un commentaire éclairant sur cette étude, v. SCHMIDT Stéphanie, « Des scientifiques ont réussi à effectuer une communication quantique contrefactuelle directe », sur *Trustmyscience.com*, 2019

force économiques interhumains sous l'effet des capacités d'usage nouvellement procurées. La régulation du marché s'adaptera probablement en conséquence.

En appliquant cette définition au cas du réseau électrique par exemple (fictif) : sur un tel réseau (i) où se nouent des relations par voie électrique, (ii) les délinquants (hacker, escrocs, auteurs de propos haineux...) empruntant un réseau quantique ne se heurtent aux mêmes obstacles ni ne possèdent les mêmes pouvoirs techniques (iii) pour imposer leurs méfaits (iv) aux autres utilisateurs du même réseau que s'ils empruntaient un réseau binaire. L'évolution de la composition interne de l'objet « réseau électrique » (quantique/binaire) entraîne une évolution des rapports de force interhumains par voie électrique sous l'effet des capacités d'usage nouvellement procurées. La régulation du réseau s'adaptera probablement en conséquence.

Aussi peut-on en tirer la conclusion suivante : **les modifications physiques internes à l'objet entraînent dans l'espace social une variation des rapports de force interhumains** tels que définis (on peut bien « parler » de rapports de force conformément à cette définition). Partant de ce constat valable pour les lois physiques, on en interrogera la validité pour le réseau internet en posant la **seconde hypothèse** que **des lois binaires internes à la machine numérique influencent les rapports de force interhumains dans l'espace social** – on l'expérimentera plus loin.

On relève par ailleurs que l'exploration de ce lien entre l'activité interne d'un objet et les rapports de force interhumains est permise par le regard endogène porté sur l'objet. On en déduit que, si des facteurs internes à la machine numérique contribuent réellement aux rapports de force interhumains *via* le réseau internet, lesdites contributions seront observables depuis ce point de vue. Cette pertinence du regard endogène pour l'étude des rapports de force interhumains en ligne n'exclut pas celle du regard exogène mais la complète, de la même manière que la physique quantique ne remet pas en cause la validité de la physique classique dans le monde macroscopique mais enrichit la compréhension de ce dernier. La question de savoir si, comment et dans quelle mesure la réalité interne d'un objet agit sur une réalité externe a parcouru les sciences du XXe siècle, d'abord celles de la Nature (physique, chimie, biologie...) puis celles sociales. On l'a remarqué en sciences littéraires, à travers la démonstration oulipo-structuraliste d'un système abrité par l'objet littéraire qui encadre et oriente la pensée du lecteur ; on l'a remarqué en ethnologie (Leroi-Gourhan), en psychologie et en ingénierie informatique, dont des scientifiques ont approfondi le rapport entre l'autonomie de la Machine et la vie humaine ; on l'a aussi remarqué en sciences juridiques, politiques, de l'information et de la communication ou en sociologie, où plusieurs auteurs identifient une vie normative interne au réseau internet emportant des conséquences humaines et des enjeux de régulation [v. *supra*]. À notre tour, le regard endogène porté par cette thèse sur internet nous amène à constater qu'une activité interne à ce réseau est animée par des lois propres configurant les données binaires en ligne comme des « prescriptions », dont l'action ainsi prescriptive influence les rapports de force interhumains *via* l'utilisabilité et l'utilisation de ce réseau.

Section 2. Les prescriptions numériques

L'observation d'une action prescriptive exercée par la donnée binaire (Paragraphe 1) ouvre sa comparaison avec d'autres types de prescriptions, à commencer par celles juridiques (Paragraphe 2).

Paragraphe 1 – L'action prescriptive de la donnée binaire

La compréhension numérique des données binaires par la machine qui les reçoit (A) dévoile une action à caractère prescriptif exercée par ces données auprès de la machine (B).

A) La compréhension machinale de l'action binaire

1. La production, la mémorisation (le « stockage ») et l'exécution des données

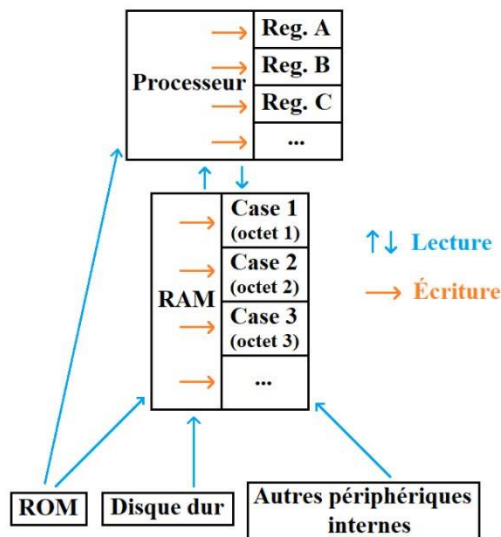
En sciences physiques et chimiques, l'action atomique des particules microscopiques, sources de toute réalité matérielle, a pu être identifiée en éprouvant les mouvements atomiques révélateurs de l'activité microscopique : les changements de vitesse particulière entre deux longueurs d'onde (H. Lorentz), la cadence des projectiles de radioactivité (E. Rutherford) ou encore la fréquence des collisions particulières (J. Perrin) ont servi à explorer cette activité microscopique afin de conceptualiser l'existence de l'atome. On s'en inspirera pour vérifier que l'action des données binaires, sources de toute activité numérique machinale, peut à son tour être identifiée en expérimentant la compréhension machinale révélatrice de l'activité interne à la machine numérique : **connaître la compréhension par la machine des données qu'elle reçoit devrait alors offrir de connaître et de qualifier l'action exercée par la donnée binaire auprès de cette machine**. Pour s'en assurer, on interrogera d'abord la compréhension machinale de la donnée binaire avant de se demander si, de cette compréhension machinale, il est ou non possible de remonter jusqu'au mode d'action de la donnée numérique.

Premièrement : comment la machine comprend-elle une donnée binaire ? On appelle « compréhension machinale d'une donnée binaire » l'intégration de cette donnée dans la mémoire de la machine. Une mémoire informatique est le support d'existence de toute donnée numérique. Une machine numérique comporte généralement plusieurs mémoires. La ROM (Read-Only Memory, ou « mémoire morte »), est une mémoire à faible capacité qui stocke le logiciel de base de la machine, à savoir le BIOS (Basic Input Output System) chargé notamment : de solliciter les différents composants matériels de la machine (l'écran, le disque dur, le clavier, l'horloge...) pour vérifier qu'ils répondent positivement à l'appel ; et de définir l'ordre dans lequel le processeur doit traiter les données³⁶⁷. Outre la ROM, le disque dur interne est une mémoire de masse qui, pour sa part, stocke notamment le système d'exploitation de la machine (Windows, Mac, Linux, Android...) ³⁶⁸. En plus de ces mémoires, la machine comporte d'autres périphériques internes tels : la carte son (qui fait circuler les signaux du son convertis en signaux numériques), la carte graphique (qui fournit l'image en faisant circuler les signaux graphiques convertis en signaux numériques par pixélisation), la carte réseau (qui fait circuler les signaux de connexion entre deux machines numériques) etc.

Lors de la mise sous tension de la machine, *i.e.* au démarrage, les mémoires (ROM, disque dur...) et autres périphériques internes (carte son, carte graphique, carte réseau...) renvoient ces données vers la mémoire vive (RAM). La RAM centralise ainsi toutes les données transférées par les périphériques internes. Le processeur n'a plus qu'à récupérer lesdites données dans la RAM pour les exécuter. Les composants matériels d'une machine peuvent se transférer entre eux les données qu'ils contiennent grâce à deux mécanismes : **la lecture et l'écriture**.

³⁶⁷Ceci se fait notamment au moyen des instructions d'interruption et d'exception qu'on examinera plus loin. Sur le fonctionnement de la ROM, v. KUMAR A. Anand, *Fundamentals of Digital Circuits*, 4e ed., PHI Learning, 2016, p. 943s.

³⁶⁸Ce rôle peut aussi être assuré par la mémoire flash

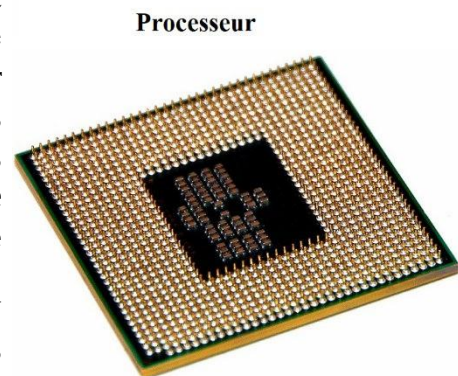
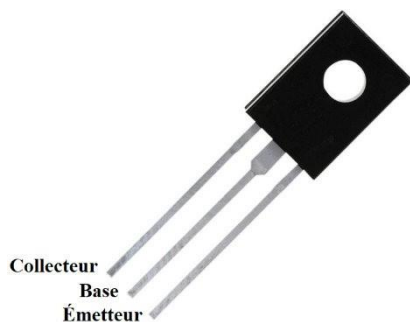


Une mémoire est lue lorsque les données qu'elle stocke sont transférées vers une autre mémoire ou vers le processeur. Toute mémoire peut être lue. Seulement, la lecture implique seulement le transfert des données, et non leur stockage par la mémoire ou le processeur récepteur. C'est là le rôle de l'écriture. Lorsqu'un composant écrit, il stocke dans son espace mémoire ou ses registres les données transférées par lecture d'une autre mémoire. Tout composant ne peut pas écrire des données. Deux composants principalement en sont capables : la RAM et le processeur. La RAM écrit les données qui lui sont transférées dans ses « cases », chaque case pouvant contenir ni plus ni moins qu'un octet (suite de 8 bits). Le processeur écrit les données qui lui sont transférées dans ses registres pour pouvoir les exécuter (les « traiter »).

La compréhension des données par la machine – i.e. leur intégration dans l'espace mémoire de la machine – se traduit donc par trois opérations : le stockage de ces données (leur conservation par la mémoire) ; leur lecture (transfert de données stockées) ; et leur écriture (stockage de données transférées). Par conséquent, **on définit la compréhension machinale comme l'ensemble des opérations de stockage, de lecture et d'écriture de données.**

La compréhension machinale des données binaires doit être distinguée de la production et de l'exécution de données. Concernant la production de données, elle consiste à produire des signaux électriques qui seront convertis en données binaires. Pour ce faire, doit d'abord être produite une séquence de décharges électriques alternées de 0V et 5V, de type 0V-5V-0V-5V-0V-5V-0V-5V-0V. Ensuite, cette suite de signaux électriques est déchargée sur des transistors (à gauche) intégrés dans la machine. La branche collectrice du transistor est reliée par sa base de rattachement à une branche émettrice qui réexpédie cette séquence vers la mémoire. Une fois que la mémoire a intégré les signaux électriques reçus, elle les stocke sous la forme de 0 (signal négatif) et de 1 (signal positif) : la séquence 0V-5V-0V-5V-0V-5V-0V-5V-0V devient alors l'octet 01010010 dans la mémoire.

Quant à l'exécution d'une donnée, elle est exclusivement mise en œuvre par le processeur. Le processeur peut effectuer **quatre types d'opérations** pour exécuter une donnée : des opérations arithmétiques (addition, soustraction, multiplication...) ; des opérations comparatives (supérieur, inférieur, égal) ; des opérations de transfert (des données figurant dans un registre vers un autre registre ou vers la RAM, des données figurant dans la RAM vers le processeur...) ; et des opérations logiques (NON, ET, OU, OU exclusif...). Par exemple, le processeur reçoit les octets 10100000 (instruction fictive) et 01010010 (lettre R).



L'instruction fictive 10100000 ordonne au processeur de transférer la lettre R depuis la mémoire vive et d'effectuer des additions sur le bits reçus, appliquant ainsi l'instruction sur la lettre R.

À l'issue de son exécution, le processeur obtient un **résultat informatique**. Par exemple, pour un processeur 8086 (commercialisé par Intel entre 1978 et 1998 et servant de base aux générations suivantes de microprocesseurs), ce résultat informatique est constitué par : des bits d'acquiescement en cas d'opération de transfert (le processeur renvoie un bit d'acquiescement positif au composant qui l'a sollicité ou un bit négatif si le transfert a échoué) ; des bits de sortie logique en cas d'opération logique (le processeur renvoie à la RAM ou à un registre spécifique le bit de sortie correspondant au(x) bit(s) d'entrée selon la fonction logique exécutée³⁶⁹) ; et de bits *flags* pour les opérations arithmétiques, logiques et pour certaines opérations de transfert (un *flag* est un bit qui sert d'indicateur en apportant une information relative à l'exécution de l'une de ces opérations³⁷⁰). Si le résultat informatique est correct, c'est-à-dire s'il correspond au résultat attendu pour les octets exécutés, alors la donnée produira les conséquences de l'instruction (affichage de la lettre R sur l'écran, envoi du message contenant la lettre R...).

On examine enfin les types de données qui peuvent être ainsi produites, comprises puis exécutées. On identifie **quatre types de données numériques : les données d'exécution** (les bits constitutifs d'un résultat informatique, qu'on vient de voir) ; **les données de caractère ; les données d'adresse ; et les données d'instruction**. Les caractères désignent les données mémorisées auxquelles sont associés des symboles. Un exemple classique est celui du codage ASCII (American Standard Code for Information Interchange). Ce codage propose 128 caractères, et ne requière

³⁶⁹ P. ex., pour la fonction NON, le bit renvoyé sera 1 si le bit d'entrée est 0 et inversement conformément à la table de vérité de la fonction NON ; pour la fonction ET, le bit renvoyé sera 1 si les deux bits d'entrée sont 11, il sera 0 si les deux bits d'entrée sont 00, 01 ou 10 ; pour la fonction OU, le bit renvoyé sera 1 si les deux bits d'entrée sont 01, 10 ou 11, il sera 0 si les deux bits d'entrée sont 00 etc. V. HYDE Randall, *Write Great Code, vol.1: Understanding the Machine*, 2e ed., No Starch Press, 2020, p. 39s.

³⁷⁰ Le registre d'état d'un microprocesseur 8086 totalise 9 flags différents, tels que : pour les opérations arithmétiques, les flags CF indiquant l'exécution d'une retenue (le bit CF est à 1 en présence d'une retenue, à 0 dans le cas contraire) ou ZF indiquant l'exécution d'un zéro ; pour les opérations comparatives, le flag PF indiquant une parité (PF est à 1 si deux valeurs binaires sont égales, il est à 0 si l'une des valeurs binaires comparées est supérieure à l'autre) ; pour le transfert d'une interruption, les flags IF indiquant l'exécution ou l'inexécution d'une interruption ou TF indiquant l'exécution d'une interruption après chaque instruction du programme ; pour le transfert d'une chaîne d'octet, telle qu'une suite de caractères constitutifs d'un message, le flag DF indiquant l'ordre (croissant ou décroissant) d'exécution des chaînes d'octets. Cours de licence en informatique intitulé « Programmation Assembleur NASM. Résumé », Université de Limoges, sur *Unilim.fr*, 2015-2016, p. 8

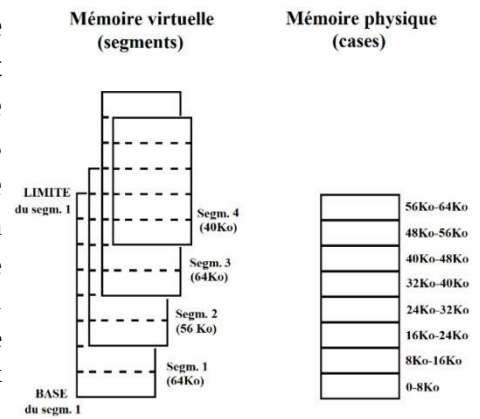
donc que 128 états binaires différents. La table de caractères est stockée sur la machine dès sa fabrication, probablement sur la ROM. Ne sont évidemment stockés sur la machine que les bits constitutifs des caractères, et non l'association de ces bits avec des caractères, dès lors que le processeur comprend seulement des bits et non des caractères. En revanche, tout logiciel permettant à l'utilisateur d'insérer des caractères (dont le système d'exploitation) se reposera sur la table des caractères pour faire correspondre l'octet 01000001 à la lettre A comme le prévoit la table. De cette façon, tous les logiciels peuvent utiliser le même octet pour produire le même caractère. Quel que soit le logiciel qu'il emploie (Windows, macOS, Facebook, Snapchat, Word...), l'utilisateur obtiendra donc chaque fois la lettre A en appuyant sur la touche A de son clavier (donc en produisant le signal 01000001).

Table de caractères ASCII		
Code base 10 (décimal)	Code base 2 (format binaire)	Caractère
0	00000000	NUL [Null, aucun signal]
1	00000001	SOH [Start of Heading, premier caractère en tête d'un message]
2	00000010	STX [Start of Text]
3	00000011	ETX [End of Text]
27	00011011	ESC [Escape]
43	00101011	+ [Plus]
63	00111111	? [Point d'interrogation]
65	01000001	A [Lettre maj. A]
97	01100001	a [Lettre min. A]
127	01111111	DEL [Delete]

Outre les caractères, les adresses désignent les données qui situent, à l'intérieur de la machine, ses composants matériels et les instructions qu'elle mémorise. Concernant d'abord les adresses des composants matériels (dites « adresses physiques »), une adresse unique est dédiée à chaque périphérique interne (ROM, disque dur, carte réseau, carte graphique, carte son...), à chaque registre du processeur, et surtout à chaque case de la mémoire vive (soit plus de 65 000 adresses réservées à la seule mémoire vive). Lorsqu'un composant doit transférer des données vers un autre composant, il lui suffit alors de préciser l'adresse du composant destinataire ; lorsque le processeur doit appeler des données – y compris des instructions – présentes dans la mémoire vive, il lui suffit de préciser les adresses des cases de la mémoire vive qui comportent les données à exécuter. Une adresse physique est constituée de 8, 16 ou 32 bits, sa taille étant limitée par le nombre de fils électriques qui relient les composants matériels et qui sont réservés au transport des données d'adresses entre les composants³⁷¹.

³⁷¹Par exemple, pour le processeur 8086, le bus d'adresses était constitué de 20 fils. Les adresses s'étendaient donc en théorie sur 20 bits mais devaient être ramenées à 16 bits pour être exécutables par le processeur (le processeur ne peut exécuter des données que par tranches de 8 bits, 16 bits, 32 bits ou 64 bits). Il existait donc 2^{16} adresses exécutables, soit 65 536 adresses exécutables.

Dès lors que le nombre d'adresses physiques est limité par les capacités matérielles de transport (bus d'adresses), ce nombre est insuffisant pour adresser chacune des instructions présentes sur les machines d'aujourd'hui. C'est pourquoi il a fallu développer des adresses logiques par-dessus les adresses physiques. L'idée est la suivante : on vient de voir que la mémoire physique est insuffisante ; les programmeurs ont donc dû créer une mémoire virtuelle à l'aide d'un logiciel ; ce logiciel donne naissance à des « segments » qui se superposent sur les cases de la mémoire physique ; chaque donnée présente dans un segment possède une adresse logique qui la situe dans ce segment. Ainsi, toute instruction possède une triple adresse : une adresse physique (plusieurs instructions peuvent partager la même adresse physique) ; une adresse linéaire (qui, une fois calculée par le processeur, permet de connaître l'adresse logique d'une instruction à partir de son adresse physique) ; et une adresse logique (une même instruction peut posséder une ou plusieurs adresses logiques mais deux instructions distinctes ne peuvent pas avoir la même adresse logique).

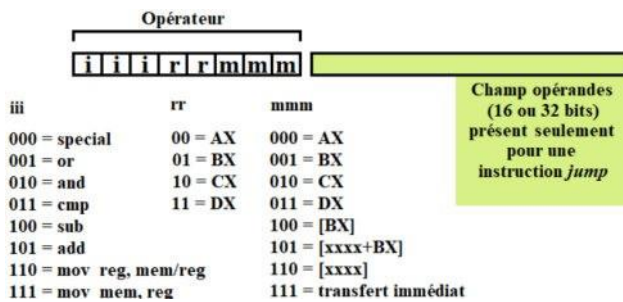


2. Les données d'instruction

Enfin, après les données d'exécution, de caractère et d'adresse, le dernier type de données qu'on identifie est l'instruction. **L'instruction est une donnée qui indique au processeur les opérations d'exécution qu'il doit effectuer.** On distingue trois catégories d'instruction : ce qu'on qualifiera dans le cadre de cette thèse les « **instructions préalables** » ; les **instructions machine** ; et les **instructions logicielles**. On appelle « instruction préalable » toute instruction antérieure aux instructions machine. Cela couvre deux sortes d'instruction : les interruptions et les exceptions. Ces instructions ont pour but de prévoir le cas dans lequel un événement spécial survient. Lorsque le processeur fait face à un événement spécial identifié par une interruption/exception, il sauvegarde les processus en cours d'exécution, en interrompt l'exécution, appelle l'adresse de l'interruption/exception concernée à son emplacement mémoire, exécute isolément cette interruption/exception, restaure le contexte d'exécution des processus interrompus et en reprend le cours. Par exemple, lorsqu'un programmeur stocke des instructions peu privilégiées dans un emplacement de la mémoire réservé à des instructions privilégiée du système d'exploitation, cela fait entrer deux processus en conflit lors de leur exécution (hypothèse prévue par l'exception INT13, dite « Défaut de protection général »). Dans ce cas, le système d'exploitation ordonne au processeur la sauvegarde des contextes des processus en cours, la suppression du processus défaillant de la file d'attente d'exécution pour mettre un terme au conflit, la poursuite de l'exécution des autres processus, et l'affichage sur l'écran d'un signal d'erreur. Parmi d'autres exceptions, INT 11 vise l'inexistence d'un segment mentionné par l'instruction, INT 8 une double faute, INT6 l'invalidité d'une instruction machine³⁷²... Comme la table des caractères est le programme qui recense les octets correspondant aux caractères, la table des interruptions (*Interrupt Descriptors Table*) est le programme stocké dans la ROM qui recense les octets correspondant aux exceptions et interruptions.

³⁷²Pour la liste des 256 exceptions et interruptions standardisée par BROWN Ralf, v. www.ctyme.com/intr/int.htm

Quant aux instructions machine, elles se distinguent des instructions préalables par la présence d'un « opérateur » qui précise au processeur le type d'opération qu'il doit effectuer lors de l'exécution. Pour un microprocesseur 8086, qui répond au jeu d'instructions x86, un



opérateur s'écrit basiquement *iiirrrmmm*³⁷³ : où *iii* = 001 pour indiquer une opération logique OU, 010 pour une opération logique ET, 011 pour une opération comparative (<, >, =), 100 pour une opération arithmétique de soustraction, 101 pour une addition, 110 pour une opération de transfert de données d'un registre du processeur vers la mémoire vive et 111 pour un transfert de la mémoire vive vers un registre ; et où *rr* et *mmm*

sont les adresses des registres du processeur subissant l'opération (registres AX, BX, CX ou DX). Grâce à cette structure, l'instruction machine peut ainsi définir des opérations arithmétiques, logiques et de transfert que doit effectuer le processeur. Le champ « opérandes » indique quant à lui les données auxquelles appliquer ces opérations – par exemple, si on souhaite faire exécuter la lettre R, le champ opérandes pourra être constitué des octets 00000001 (premier caractère en tête d'un message) 01010010 (lettre R), sur lesquels seront appliqués les opérations mentionnées dans l'opérateur³⁷⁴.

Enfin, on appelle « instructions logicielles » l'ensemble des instructions rédigées dans un langage humainement compréhensible et destinées à faire exécuter des instructions machine et/ou des instructions préalables. Pour faciliter le recours à une instruction machine, le programmeur lui appose un symbole appelé « mnémonique ». Les mnémoniques désignant spécifiquement l'opérateur d'une instruction machine sont surnommées « opcode ». Par exemple, les instructions machine ordonnant un transfert de données (en lecture ou écriture, de 8 ou de 32 bits) s'identifient par l'opcode MOV ; les instructions machines ordonnant une addition (immédiate ou non, en lecture ou en écriture, de 8 ou de 32 bits) s'identifient par l'opcode ADD etc. La correspondance entre des mnémoniques et les bits constitutifs des instructions machine est établie par un programme dit « assembleur ». L'utilisation de l'assembleur par un programmeur permet alors de traduire les mnémoniques qu'il utilise en instructions machines sous leur format binaire.

En combinant plusieurs mnémoniques, un langage informatique permet ainsi de combiner plusieurs instructions machines pour créer de nouvelles fonctions. Par exemple, obtenir l'adresse effective d'une instruction (*i.e.* la triple adresse physique/linéaire/logique) nécessite en principe plusieurs instructions machine de calcul (instructions ADD et MUL pour additionner et

³⁷³On reprend ce schéma de HYDE R., *Write Great Code, vol.1: Understanding the Machine*, préc., p. 293s

³⁷⁴Le champ « opérandes » ne sera rempli que si les données auxquelles appliquer l'opération se situent l'une après l'autre, c'est-à-dire si les adresses de ces données se succèdent dans la mémoire vive. En effet, le processeur exécute en principe les données les unes après les autres, dans l'ordre de leur stockage par la mémoire vive. Dans ce cas, il n'est nul besoin de préciser les données à exécuter : elles le seront automatiquement l'une après l'autre. En revanche, lorsque les données ne se succèdent pas, il est nécessaire de préciser dans le champ opérandes les données auxquelles appliquer l'opération, ce qui traduit l'obligation pour le processeur de faire un « saut » (fonction *jump*) dans la mémoire pour récupérer les données concernées.

multiplier différents bits) et de transfert (instructions MOV pour la lecture et l'écriture des adresses pertinentes)³⁷⁵. Pour éviter au programmeur d'introduire chacune de ces mnémoniques pour chaque instruction appelée, le langage de l'assembleur propose la fonction LEA (*Load Effective Address*). Il suffit alors au programmeur d'utiliser la mnémonique LEA pour combiner toutes les instructions machines (ADD, MUL, MOV...) nécessaires à l'obtention de l'adresse effective d'une instruction. Ainsi, on peut écrire en langage assembleur la formule suivante pour demander au processeur d'exécuter l'ordre de dessiner un pixel sur l'écran :

lea esi, INT 10h	// obtention de l'adresse effective de l'interruption INT 16 via le registre esi du processeur. INT 16 est ici notée en hexadécimal (10h) comme c'est l'usage. Cette interruption est dédiée à la reconnaissance graphique
mov eax, [esi]	// lecture par le registre eax (réservé au traitement des instructions et caractères de 32 bits) de l'instruction dont l'adresse est contenue dans esi (registre réservé au traitement des offset de 32 bits) vers le registre eax
add ah, 12	// incrémente immédiatement la valeur 12 dans le registre ah (réservé aux opérations arithmétiques pour les données de 8 bits). Concernant la valeur 12, la plupart des interruptions se décomposent en plusieurs fonctions. INT16 se décline en 19 fonctions, telles « changer la forme du curseur (fonction n°1), « définir la position du curseur » (n°2) etc. « Dessiner un pixel » est la fonction n° 12 d'INT16. On ajoute donc la valeur 12 (qui s'écrit 00001100, sur 8 bits, d'où la pertinence du registre ah).
mov [esi], eax	// écriture de l'instruction par esi depuis eax

Un langage informatique supérieur au langage de l'assembleur pourra évidemment, à son tour, combiner l'ensemble de ces mnémoniques en un seul mnémonique ou une seule fonction et ainsi de suite. La combinaison des instructions logicielles permet ainsi de superposer des instructions par-dessus d'autres, et de créer un nombre théoriquement illimité de nouvelles fonctions - de la même manière que le mnémonique LEA permet de créer la fonction « obtenir l'adresse effective d'une instruction ». En somme, le langage machine (compréhensible uniquement par le processeur de la machine et constitué des données de caractère et d'adresse, des instructions préalables et instructions machine) est superposé par des langages logiciels bas niveau (compréhensibles par l'être humain, tel le langage assembleur), qui sont eux-mêmes superposés par des langages haut niveau. Plus le langage est haut, plus il s'abstrait du langage machine : certains langages hybrides combinent le bas et le haut niveau (manipulant des instructions machine et des fonctions logicielles : langages C, C++, C#...) ; d'autres langages purement fonctionnels se hissent au plus haut niveau d'abstraction et offrent de grandes possibilités de programmation (manipulant exclusivement des fonctions logicielles : Javascript, Python, Java, Ruby...). Les langages haut niveau vont ainsi puiser dans

³⁷⁵ Les données d'adresse à additionner ou à multiplier concernent principalement les bits qui identifient le segment où se trouve l'instruction recherché (adresse segment) avec les bits constitutifs de l'espace qui sépare la présence de l'instruction dans la mémoire virtuelle et la mémoire physique (espace appelé « déplacement », ou « offset »). Quant aux données d'adresse qui doivent être lues et écrites pour obtenir une adresse effective, il s'agit des données d'adresse du segment et/ou de celles constitutives du couple segment:offset.

les ressources des langages bas niveau et machine pour proposer de nouvelles fonctions aux programmeurs et, *in fine*, aux utilisateurs.

B) Le mode d'action prescriptif de l'ordre binaire

Deuxièmement : la compréhension machinale de la donnée binaire permet-elle de remonter jusqu'au mode d'action d'une telle donnée ? La donnée porteuse d'une instruction machine étant comprise *comme un ordre* par la machine, on peut certes déjà en déduire qu'elle agit *comme un ordre* auprès de cette machine. Mais de quel type d'ordre est-il question ? Un ordre peut être contraignant ou non-contraignant, général ou particulier, direct ou mandaté... Outre le format binaire de l'ordre émis par instruction machine, on ignore encore les caractéristiques de son mode opératoire. Aussi nous appartient-il ici d'approfondir ces caractéristiques opérationnelles de la donnée numérique dans le but de qualifier précisément la manière dont elle agit en tant qu' « ordre binaire » (*i.e.* en tant qu'elle est porteuse d'une instruction machine).

La compréhension de la donnée comme un ordre à exécuter par la machine numérique nous ramène d'emblée – influencés par notre regard de juriste – à des caractéristiques « prescriptives ». D'après le vocabulaire juridique, le mot « prescription » est communément employé pour convoquer une règle telle qu'ordonnée par le producteur de droit – que la règle soit générale (sujétion de personnes collectivement désignées à des exigences légales, constitutionnelles, administratives...) ou individuelle (sujétion de personnes individuellement désignées à des expertises, enquêtes, décisions *inter partes*...), que cette règle soit produite au nom du fait (coutume, convention politique/sociale...) ou d'un statut (loi adoptée par le législateur et promulguée par le Président de la République, jurisprudence rendue par le juge, décret édicté par le gouvernement...)³⁷⁶. Trois conditions définitoires sont alors constitutives d'une prescription juridique, d'une « règle telle qu'ordonnée par le producteur de droit » : l'énonciation d'une règle de droit (condition de formulation de la prescription) ; l'émission d'un ordre d'exécuter cette règle (condition d'activation de la prescription) ; et l'exécutabilité de ladite règle (condition d'application de la prescription). On retrouve donc les trois niveaux d'action d'un ordre binaire, qui a pour effet de déclencher une règle énoncée par langage machine en adressant une instruction machine exécutable. L'ordre binaire et la prescription juridique trouvent tous deux leur réalisation en suivant un même processus (énonciation de la règle/ordre d'exécution/exécution).

Ce processus commun de réalisation ne suffit pas pour autant à conclure au caractère prescriptif d'un ordre binaire, ce pour plusieurs raisons. Déjà, le fait que l'ordre binaire suive le même processus que la prescription juridique ne prouve pas que ce processus est proprement prescriptif. Au surplus, un processus communément suivi par deux objets ne permet pas d'en déduire une similitude des objets : de l'eau liquide (dans une fontaine) et du sable solide (dans un sablier) adoptent communément un processus d'écoulement, sans que l'on puisse dire du premier qu'il est du sable ou qu'il est solide ; de la même manière, on ne saurait tenir l'ordre binaire pour une prescription du seul fait qu'il partage un processus commun avec la prescription

³⁷⁶CORNU Gérard, *Vocabulaire juridique*, Entrée « Prescrire », sens n° 2 (générique) : « *plus généralement, établir une règle* » ; sens n° 3 : « *ordonner, enjoindre, commander (s'agissant non plus d'une règle générale mais d'une décision individuelle)* ». Entrée « Prescription », sens n° 5 (générique) : « *plus généralement, parfois synonyme de règle* ». Entrée « Règle », sens n° 1 : « *désigne toute norme juridiquement obligatoire (normalement assortie de la contrainte étatique), quels que soient sa source (règle légale, coutumière), son degré de généralité (règle générale, spéciale), sa portée (règle absolue, rigide, souple) etc.* »

juridique. Enfin, comme on le constatera au moment de comparer l'ordre binaire avec la prescription juridique [*infra*], ce processus « commun » se réalise en fait très différemment pour la première (produite et exécutée numériquement) et la seconde (produite et exécutée humainement), et on ignore à ce stade combien ces différences affectent la ressemblance entre les deux objets. Pour ces raisons, le processus de réalisation d'une prescription juridique est si aligné sur le Droit et son fonctionnement qu'il est ici difficile de pousser plus loin l'analogie avec l'ordre binaire.

Néanmoins, le constat d'un processus commun avec la prescription juridique ouvre la piste d'un possible caractère prescriptif attaché à l'ordre binaire. Pour savoir quel crédit donner à cette piste, il nous faut alors vérifier si la ressemblance d'un ordre binaire avec une prescription juridique est une coïncidence processuelle (tels l'eau et le sable), ou si l'ordre binaire correspond substantiellement à une prescription plus générique – ce qui nous oblige à quitter l'exemple particulier de la prescription juridique pour nous référer à un vocabulaire plus courant. La racine étymologique du mot « prescription » nous aidera, une fois encore, à en baliser le périmètre lexical. En latin, composé du préfixe *præ* (avant) et du verbe *scribere* (écrire), le supin *præscriptum* se rapporte à une caractéristique antérieure au support (écrit à l'origine, immatériel par extension). L'évolution latine du verbe *præscribo* est retracée par le dictionnaire Gaffiot³⁷⁷ : de la signification primitive « *mettre en titre* » en a découlé celle de « *mentionner d'avance* » (par ex. « *indiquer d'avance au sénat quelles guerres il faut faire* »). Le sens a par ailleurs glissé vers une *préparation*, une *planification* (« *tracer d'avance le plan de son futur règne* » incluant l'action de tracer des limites), avant de s'orienter vers la *présentation* d'un garant et l'*octroi* de garanties (par ex. « *des droits à ses citoyens* » ou « *prescrire à qqun les moyens de se guérir* »). Pour chacune de ces situations, la prescription désigne une décision abstraite (celle d'intituler, d'aviser le sénat, de conquérir/régir, de garantir, de soigner) qui trouve un support concret d'existence (un ouvrage, un discours ou un écrit, un acte de conquête, une loi, une ordonnance médicale).

Encore que toute décision mise en support n'est pas constitutive d'une prescription : comme le précisent les dictionnaires modernes de la langue française, la prescription énonce non une simple « règle » mais une « *règle à suivre* »³⁷⁸, une « *règle de conduite* »³⁷⁹, i.e. une règle dont l'issue prévue est celle d'un *suivi* de cette règle, de l'observation d'une *conduite*, en somme d'une *conformité* à ce qu'énonce la règle. Suivant ces définitions, une décision mise en support n'acquière alors de caractère prescriptif qu'en satisfaisant deux fonctions : (i) la création d'une règle ; et (ii) l'exigence d'une conformité à la règle. Sur la première fonction, en rappelant les travaux d'A. Ross, une règle est créée dès lors qu'un fait déterminé F et une conséquence C sont corrélés au moyen d'un conditionnement. En ce sens, **toute « règle » peut être notée « F → C », où la survenance de F conditionne celle de C** (et en constitue ainsi la cause) **et où « → » désigne un rapport de conditionnement entre F et C**. Sur la deuxième fonction, celle de l'exigence de conformité, elle suppose à la fois la formulation d'un ordre porteur de la règle³⁸⁰ (ordre qui incarne l'exigence) et la potentialité de faire respecter cet ordre et la règle qu'il porte

377Dictionnaire Gaffiot, Entrées « *Præscriptum* », « *Præscribo* » et « *Præscriptio* » [en ligne]

378Dict. du CNRTL, Entrée « *Prescription* », sens B, n° 1 [en ligne]

379Dict. Larousse, Entrée « *Prescrire* », sens n° 1 : « *donner comme ordre, (...) comme règle de conduite* »

380Dict. Larousse, Entrée « *Prescription* », sens n° 1 : « *ordre formel et détaillé énumérant ce qu'il faut faire* ». Dict. Littré, Entrée « *Prescrire* », sens n° 1 : « *ordonner, commander* ». Dict. du CNRTL, Entrée « *Prescription* », sens B, n°1 : « *commandement, précepte* » ; sens B, n° 2 : « *ordre formel, catégorique* ».

(potentialité qui incarne la faisabilité d'une mise en *conformité*). En ce sens, « exiger la conformité à une règle » équivaut à « ordonner le respect d'une règle ». Cumulant ces fonctions, une prescription est (i) une règle mise en support (ii) dont il est possible d'ordonner le respect. Ne sont donc pas qualifiables de prescriptions : (i) la donnée binaire, qui met en support la décision de produire des données mais qui ne porte aucune règle d'ici à rencontrer le langage machine ; (ii) les travaux préparatoires du Parlement, qui mettent en support les décisions issues d'un débat mais qui ne posent aucune exigence de conformité auxdites décisions.

Si l'exigence de conformité est indispensable à la prescription, c'est parce qu'une règle inapte à toute concrétisation ne peut être une règle *suivable*, applicable à une *conduite*, et ne remplirait donc pas les critères définitoires précités. En d'autres termes, une règle est abstraitement qualifiable de prescription avant tout respect concrétisé – une disposition légale est « prescription » avant sa mise en œuvre par le juge et les agents de l'administration, tout comme une ordonnance médicale est « prescription » avant la délivrance du médicament par le pharmacien. Du moment que le respect d'une règle est assorti d'un moyen de concrétisation potentielle, cette règle vaut prescription. Plus exactement, l'aptitude d'une règle à obtenir concrétisation dépend de deux mécanismes : un mécanisme d'exécution et un mécanisme d'application. S'agissant de l'exécution, le dictionnaire Gaffiot rappelle que l'étymologie latine de ce mot renvoyait déjà, quasiment exclusivement d'ailleurs, à l'idée d'un « suivi », particulièrement du suivi d'une règle de droit par l'institution judiciaire³⁸¹. Dans la continuité de cette signification, on considèrera alors l'exécutant comme celui qui assure le suivi concret d'une règle, qui valide la concrétisation de cette règle.

En ces termes, le mécanisme d'**exécution de la règle** a pour rôle de **la valider** (ou de l'invalider), *i.e.* de **confirmer** (ou d'infirmer) **le caractère prescriptif de la règle dans un cas concret**. Comme on le détaillera, la validation implique à la fois que soit confirmée l'inclusion de cette règle dans le système prescriptif (par ex., système juridique ou système médical) gardé par l'exécutant (par ex. le juge ou le pharmacien) et que la prescription dépasse sa qualification abstraite en étant confrontée à une situation de fait à laquelle s'appliquer. À l'issue de l'acte d'exécution, on sait donc que la règle invoquée est *comprise* par ce système en qualité de prescription, et qu'elle peut ainsi trouver application dans ce même système. Le mécanisme d'**application de la règle** a quant à lui pour rôle de **l'accomplir**, *i.e.* de la réaliser dans le ressort (généralement physique) du destinataire de la règle (*i.e.* de celui désigné par la règle pour supporter la conséquence C prévue, tel l'auteur d'une infraction ou le patient nécessitant un traitement) concerné par la décision de l'applicateur (par ex., l'administration pénitentiaire qui applique une peine d'incarcération ou le pharmacien, exécutant et applicateur, qui délivre les médicaments prescrits). À l'issue de l'acte d'application, la règle aboutit sa concrétisation. *Via* ces deux mécanismes, une règle existant abstraitement peut être traduite physiquement après qu'ait été émis l'ordre de son application. Pour renfermer une exigence de conformité et muer en prescription, une règle doit alors être reliée par un ordre à une hypothèse de concrétisation – autrement dit être aussi bien exécutable (par validation) et applicable (par accomplissement) sur injonction.

On déduit de ces considérations une **définition définitive d'une prescription** comme étant **une règle exécutable et applicable dont la réalisation procède d'un ordre contraignant**. La

³⁸¹L'exsēcūtō (« 1. Achèvement, exécution (...) 3. Poursuite judiciaire ») et l'exsēcūtōr (« 1. Celui qui exécute. 2. Tout magistrat chargé d'exercer des poursuites [sens employé par le Code Justinien]. 3. Celui qui poursuit qui venge, vengeur ») dérivent ainsi du verbe exsēquor (« suivre jusqu'au bout ») : Dict. Gaffiot, Entrée « exécution »

prescription satisfait ainsi : (a) la fonction d'exiger la conformité à une règle ; (b) la finalité de voir cette règle appliquée ; (c) et un mode opératoire injonctif. L'ordre binaire (l'instruction machine) s'insère-t-il dans cette définition de la prescription ? À ce stade de l'étude, il est encore trop tôt pour déterminer si l'instruction machine a la nature d'une prescription, mais du moins observe-t-on qu'elle est incontournable pour l'accomplissement d'une prescription. Rappelons que le langage machine crée une règle, fait naître un rapport $F \rightarrow C$ en attribuant à une donnée, à un « fait » binaire F une conséquence machinale C : si F (par ex., 01100100) alors C (par ex., application des fonctionnalités de la touche R par le processeur). Le processeur ne concrétise cette règle qu'après avoir été sollicité par l'instruction machine. Par conséquent, d'une part, l'instruction machine est porteuse d'une règle créée (par langage machine), exécutable et applicable (par le processeur), *i.e.* d'une prescription. D'autre part, l'instruction machine est l'ordre par lequel cette règle peut trouver concrétisation. L'instruction machine permet ainsi à la règle posée par le langage machine : (a) de concrétiser l'exigence de conformité que renferme cette règle en étant effectivement associée à un mécanisme d'exécution et d'application ; (b) de déboucher sur une application de cette règle ; (c) et ce par voie injonctive, à savoir par l'émission d'un ordre. Par son rôle, l'instruction machine est l'élément numérique grâce auquel une telle règle peut réaliser les fonction, finalité et mode opératoire caractéristiques d'une prescription. Dans notre définition de la prescription (« règle exécutable et applicable dont l'accomplissement procède d'un ordre »), l'instruction machine occupe donc la place de « l'ordre » : son action emporte des effets prescriptifs en ce sens qu'elle provoque la concrétisation d'une règle exécutable et applicable.

On peut ainsi apporter une réponse à la question : quel est le mode d'action d'une donnée binaire telle qu'elle est comprise par la machine numérique ? **À travers l'instruction machine, la donnée binaire produite exerce une action prescriptive auprès de la machine numérique** en déclenchant la concrétisation d'une prescription (*i.e.* d'une règle exécutable et applicable issue d'un langage informatique). Lorsqu'il reçoit une instruction machine impulsée par une production de données, le processeur reçoit donc des prescriptions *numériques*, comprises comme « prescriptions » par la seule machine *numérique* et appelant exécution et application de sa part.

Identifiées comme telles, ces **prescriptions numériques, ces règles créées par langage informatique, exécutables et applicables par une machine numérique et dont l'accomplissement procède d'une instruction machine**, deviennent comparables aux prescriptions juridiques avec lesquelles elles partagent la caractéristique prescriptive. Au vu de ces explications, il apparaît de moins en moins que les points communs soulevés entre le processus de réalisation d'une donnée binaire et celui d'une prescription juridique relèveraient d'une coïncidence processuelle (tels l'eau et le sable). Ordre binaire et prescription juridique semblent tous deux s'insérer dans un processus proprement prescriptif. Si cette supposition se vérifie, l'existence de prescriptions numériques constatée sur le plan substantiel (définition de la « prescription » communément valable pour la règle de droit et pour la règle formulée par langage machine) pourrait être confirmée sur le plan fonctionnel (processus commun de réalisation des prescriptions étatique et numérique).

Paragraphe 2 – Comparaison des processus prescriptifs juridico-étatique et numérique

En modélisant le processus suivi par une règle de droit afin de se réaliser en tant que prescription juridico-étatique (A), on note que les mêmes étapes prescriptives sont suivies par le processus dans lequel s'inscrit une production de données d'ici à sa réalisation numérique (B).

A) Modélisation simple du processus prescriptif juridico-étatique

On comparera ici la règle de droit avec la règle formulée par langage machine. On s'inspirera à ce titre de la méthodologie comparative proposée par Guillaume Tusseau (v. Introduction), d'après laquelle deux concepts doivent être comparés à l'aune d'un métaconcept - telles une carotte et une pomme de terre comparées à l'aune du métaconcept « légume », « couleur de l'objet », « goût de l'aliment » etc. Dans notre cas, pour comparer la règle de droit et la règle issue du langage machine, on se référera au méta-concept de « prescription ». Ce choix n'est évidemment pas aléatoire, puisqu'on a déjà établi que ces deux types de règles obéissent à une même substance sémantique de la prescription, à savoir une règle exécutable et applicable dont l'accomplissement procède d'un ordre. Par ailleurs, à notre connaissance, il n'est pas aujourd'hui contesté qu'une règle de droit est constitutive d'une prescription. Plus admise que la « prescription numérique », la prescription juridique nous servira de point de départ pour décortiquer le processus qu'elle emprunte pour se réaliser en tant que prescription. En comparant le déroulement de ce processus avec celui suivi par une règle de langage machine pour se réaliser, on devient en mesure non seulement de confirmer ou d'infirmer la pertinence du terme « prescription » pour qualifier cette règle sur le plan de son fonctionnement, mais aussi de noter les différences entre ces processus juridique et numérique.

Pour rappel, dans le cadre de ce travail, nous avons restreint le périmètre du « Droit » au seul périmètre étatique. La « règle de droit » n'est donc prise ici que dans le sens d'une règle reconnue comme telle par l'État. Cette restriction s'explique par notre objet d'étude, porté sur l'analyse des rapports de force entre l'État (*via* l'outil juridique) et les acteurs d'internet (*via* l'outil numérique). Afin de préciser les éléments concernés par cette comparaison, on préférera donc l'adjectif « étatique » à celui de « juridique » pour désigner une prescription couverte par une règle de droit telle que reconnue par l'État. Quelles sont alors les étapes parcourues par cette règle de droit pour se réaliser en tant que prescription étatique ? Que se passe-t-il entre le moment où est énoncée la règle de droit et celui où elle est appliquée physiquement ?

1^{ère} étape : la création d'une règle abstraite. Acte de naissance de toute prescription, l'énonciation d'une règle rigide R_R consiste à créer un rapport de conditionnement $F \rightarrow C$, en sorte que $R_R = F \rightarrow C$ quel que soit R_R . Si R_R est une règle légale, c'est le législateur qui sera chargé par l'État de l'énoncer en créant un rapport $F \rightarrow C$; si R_R est une règle constitutionnelle, elle sera énoncée par le constituant ; si R_R est une règle jurisprudentielle, $F \rightarrow C$ sera posé par le juge etc. Sans omettre les autres prescriptions étatiques, on se concentrera sur la règle légale (la *loi*) pour expérimenter le processus prescriptif étatique. À ce premier stade, la règle est entièrement abstraite, elle ne rencontre aucun cas concret auquel s'appliquer ; elle se borne à conditionner la provocation d'une conséquence théorique par la survenance potentielle d'un fait.

2^e étape : l'association de la règle à une exigence abstraite de conformité. Seulement après avoir été posée, la règle de droit créée sur habilitation étatique devient potentiellement réalisable. Cette potentialité est acquise par l'association de la règle de droit à un mécanisme préexistant d'exécution et d'application. À titre d'exemple, en tant qu'elle est *légale*, et par ce seul statut abstrait, une règle est associée à des mécanismes préexistants d'exécution et d'application étatiques (tels respectivement un juge et une administration mettant en œuvre la décision de ce juge). Cette association découle certes d'un statut par essence abstrait mais, aussi abstraite soit cette association, elle rend la règle exécutable et applicable. Par cette association, avant même

que s'activent les mécanismes d'exécution et d'application, la règle comporte donc une exigence abstraite de conformité, *i.e.* une demande générique de son exécution et un ordre tout aussi générique de son application, hors de tout cas concret ayant effectivement eu lieu. On peut alors dire de toute loi qu'elle renferme une exigence abstraite de conformité du fait de sa légalité. À ce stade précis du processus, la règle devient apte à obtenir concrétisation grâce à son exigence de conformité et devient qualifiable de « prescription », bien que cette prescription demeure dans un état encore abstrait.

3^e étape : la rencontre de la règle avec un cas concret. Seulement après que la règle de droit est devenue exécutable et applicable, sa concrétisation peut être sollicitée en sa qualité de prescription. Ici peut démarrer la phase « concrète » d'une prescription à l'initiative d'une intervention factuelle. Plus exactement, une intervention factuelle extérieure à la règle prétend correspondre au F de ladite règle, appelant en conséquence la concrétisation de $F \rightarrow C$. La nécessité de cette intervention factuelle (*i.e.* de tout fait dont est prétendue la correspondance avec le F de la règle) s'explique par la structure même de la règle, comme l'illustre à nouveau la règle légale. Prenons la loi pénale où F représente les éléments constitutifs d'une infraction (disons un discours haineux) et où C représente la peine encourue (un emprisonnement et une amende) : C étant conditionné par la survenance de F, la conséquence C (une peine) ne peut s'appliquer concrètement que si le fait F (un discours haineux) est rempli par une intervention factuelle concrète (des propos tenus). Par la structure même d'un rapport $F \rightarrow C$, il est donc nécessaire qu'une intervention factuelle surgisse, prétende correspondre à F pour solliciter la concrétisation de $F \rightarrow C$. Aussi en déduit-on que la sollicitation pour que soit concrétisée une règle découle d'une correspondance *prétendue* devant l'exécutant, et non encore *établie* par lui, entre une intervention factuelle et F. Sur ces considérations, on définira la « sollicitation » comme l'appel déclencheur d'un mécanisme préexistant d'exécution. Dans notre illustration de la loi pénale, cette sollicitation prend classiquement la forme d'une saisine du juge judiciaire (par un justiciable ou un Procureur). On voit deux intérêts à cette sollicitation pour la réalisation d'une prescription. D'une part, croisée avec une intervention factuelle (par ex. des propos tenus), la sollicitation (par ex. une saisine du juge) forme le cas concret (par ex. un litige) dans le cadre duquel la règle est appelée à être exécutée et appliquée. D'autre part, cette sollicitation *matérialise* par un acte (par ex. saisine) une exigence de conformité jusqu'alors *abstraitemment* portée par la règle³⁸². Ce faisant, la sollicitation concrétise la demande d'exécution incluse dans cette règle et ouvre l'étape suivante.

4^e étape : l'exécution de la règle dans un cas concret. Seulement après avoir été sollicitée par une demande d'exécution dans un cas concret, la règle peut être exécutée pour ce cas. On a déjà délimité le rôle de l'exécutant à une confirmation (validation) ou une infirmation (invalidation) du caractère prescriptif de la règle dans un cas concret. Par ce rôle de validation, il arrête un état prescriptif incertain. Or, au moment où la règle de droit parvient à l'exécutant, il existe trois incertitudes sur son état prescriptif dans le cas concret : la règle invoquée peut-elle être exécutée dans le cas concret ? Trouve-t-elle exécution dans ce cas concret ? Et peut-elle s'y appliquer ?

382 Si l'exemple ici choisi de la saisine du juge fait voir une intervention factuelle antérieure à la sollicitation, l'intervention factuelle (tout fait dont est prétendue la correspondance avec F) n'est pas une notion chronologique et ne précède donc pas nécessairement la sollicitation comme on le remarquera *infra*

La première incertitude est due à une concrétisation *sollicitée* de la règle, donc non encore *obtenue*. Pour arrêter l'incertitude sur le sort de cette sollicitation, l'exécutant doit alors fixer soit la possibilité (validation de la sollicitation), soit l'impossibilité (invalidation de la sollicitation) de concrétiser la règle dans le cas concret. Lorsque l'exécutant étatique est un juge, ce problème est résolu sur le terrain de la recevabilité : la sollicitation (saisine) est valide si son expression (requête) respecte les conditions de recevabilité gardées par l'exécutant (capacité juridique, intérêt à agir, personnalité juridique, statut de victime...) ³⁸³, et la règle peut alors être concrétisée dans le cas d'espèce ; inversement, la sollicitation sera invalide si son expression ne respecte pas lesdites conditions de recevabilité, et la règle ne peut alors être concrétisée en l'espèce. Néanmoins, au terme de cette validation, on en déduit seulement que la règle *peut* être concrétisée, ce qui ne permet pas de lever la deuxième incertitude quant à savoir si elle *trouve* concrétisation.

Cette deuxième incertitude est due à l'antériorité de la 2^e étape par rapport à la 3^e : une règle peut acquérir les caractéristiques abstraites d'une prescription (en 2^e étape) avant que l'on sache si cette règle est dotée d'une valeur prescriptive dans le cas concret (survenu en 3^e étape). À nouveau, il doit donc y avoir validation, interruption du doute, ou plutôt des doutes : la règle vaut-elle prescription dans le cas concret ? Et a-t-elle pour objet de s'appliquer au cas concret ?

Pour déterminer si la règle invoquée vaut prescription, rappelons que la capacité d'une règle à être ainsi qualifiée dépend de l'exigence de conformité acquise par cette règle lors de son association abstraite avec des mécanismes préexistants d'exécution et d'application (en étape 2). Par conséquent, cette exigence ne vaut que pour ces mécanismes : si le mécanisme d'exécution associé à la règle abstraite diffère de l'exécutant effectivement sollicité pour concrétiser cette règle, l'exigence de conformité ne vaut pas pour cet exécutant. L'exigence de conformité étant un trait constitutif de toute prescription, l'exécutant qui ne reconnaît pas cette exigence dans la règle invoquée ne peut donc y voir une prescription. Gardons notre exemple du juge judiciaire français, exécutant de la loi pénale, devant qui est invoquée une règle dans un cas concret. Ce juge ne sera pas en mesure de reconnaître la moindre exigence de conformité si cette dernière ne vaut pas pour lui, *i.e.* si la règle invoquée devant lui est associée à un mécanisme d'exécution étranger à l'exécutant pénal français sollicité (une loi égyptienne associée à un mécanisme égyptien d'exécution, un pacte international associé à un mécanisme onusien d'exécution, un acte administratif associé à un mécanisme administratif d'exécution, une règle issue d'un langage machine associée à un mécanisme numérique d'exécution etc.), ou si cette règle ne respecte pas les conditions pour être associée à un

³⁸³Notons que les conditions de recevabilité peuvent varier d'un juge à un autre. Par ex., en droit français, à l'exception des personnes morales, la personne physique requérante doit en principe justifier devant le juge civil d'un intérêt à agir légitime, né, actuel, direct ou par ricochet, mais surtout personnel (ce qui implique une certitude du dommage effectivement subi par la personne du requérant, même en qualité de victime par ricochet). Inversement, devant la Cour EDH, la victime justifie d'un intérêt à agir si le dommage qu'elle prétend subir est potentiel (par ex., n'importe quel citoyen a intérêt à agir contre une loi autorisant la surveillance des administrés par le renseignement en qualité de victime potentielle de l'application de cette loi : Cour EDH, Plén., *Klass c. Allemagne*, 6 sept. 1978, n° 5029/71) ou si la cause qu'elle représente relève d'un « *intérêt général (...) qui dépasse la personne et les intérêts du requérant* » (en l'espèce, la requête d'une personne homosexuelle ayant perdu son conjoint dont il demande à récupérer le bail, et que la Cour juge recevable au nom d'un intérêt général indéfini, à défaut de pouvoir reconnaître le requérant comme victime personnelle et directe sans forcer l'Autriche à légiférer sur le droit des homosexuels à se marier : Cour EDH, 1^{re} sect., *Karner c. Autriche*, 24 juil. 2003, n° 40016/98, §24-28)

mécanisme pénal français d'exécution (défaut de promulgation, d'exequatur, de transposition...) ³⁸⁴. Inversement, un alignement du mécanisme d'exécution associé à la règle (loi pénale française correctement promulguée) et de l'exécutant sollicité pour la concrétiser (juge judiciaire français) permet à cet exécutant de reconnaître la règle invoquée en qualité de prescription.

Reconnaître la valeur prescriptive d'une règle dans un cas concret ne permet toutefois pas d'en déduire que la règle a *pour objet* de s'appliquer à ce cas. Par « objet de la règle », on désigne ici les caractéristiques (le but de la règle, ses effets, son rôle, sa fonction, ses modalités...) sous lesquelles la règle est ramenée à une unité indissociable $F \rightarrow C$. Classiquement, lorsque sont invoquées deux règles de droit contraires, chacune d'entre elles est généralement ramenée à l'objet « norme », *i.e.* à une unité normative qui indique leur rang hiérarchique respectif : une règle de droit regardée comme une norme constitutionnelle s'impose hiérarchiquement à une règle de droit regardée comme une norme légale, de rang inférieur. Il n'est toutefois pas rare que les circonstances du cas concret fassent voir à l'exécutant un tout autre objet de la règle que celui d'une « norme », auquel cas son rang normatif n'a plus de valeur dans le cas concret. On l'observe par exemple en 2016, après que le Conseil constitutionnel français eut déclaré contraire à la Constitution les dispositions légales régissant les premières semaines de perquisitions administratives durant l'état d'urgence, dont l'imprécision n'offrait pas les garanties suffisantes préserver le droit au respect de la vie privée, l'inviolabilité du domicile et le droit à un recours juridictionnel effectif issus de l'article 2 de la Déclaration de 1789. Malgré la déclaration d'inconstitutionnalité, le Conseil en annihile aussitôt l'effet prescriptif, considérant que cette inconstitutionnalité ne saurait juridiquement fonder une contestation des perquisitions menées eu égard aux nécessités d'« *ordre public* » en jeu dans le cadre de l'état d'urgence institué contre la menace terroriste ³⁸⁵. Les perquisitions menées survivant à leur inconstitutionnalité, l'art. 2 de la Déclaration de 1789 ne trouve pas ici d'application concrète auprès de son destinataire chargé de supporter la conséquence C (l'État). La valeur prescriptive de la règle constitutionnelle invoquée (art. 2 de la Déclaration de 1789) n'est pas déniée, mais cette

³⁸⁴Notons que les conditions dans lesquelles une règle est reconnue alignée sur le mécanisme d'exécution sollicité peuvent être rigides ou au contraire souples. On les qualifie de rigides lorsqu'elles sont formalisées par une procédure à suivre : promulgation, publication au JO, transposition, *exequatur*... On leur reconnaît au contraire une certaine souplesse lorsqu'elles sont conceptualisées par l'appréciation de l'exécutant. Par exemple, le seul fait que le champ matériel d'une règle de droit international associée à un mécanisme d'exécution (par ex. la Convention relative aux droits de l'enfant du 20 novembre 1989 gardé par le Comité onusien des droits de l'enfant) avoisine celui d'une règle de droit international associée à un autre mécanisme d'exécution (par ex., la Conv. EDH gardée par la Cour EDH) peut suffire à l'exécutant sollicité (par ex. la Cour EDH) pour considérer que la première règle est alignée sur un même mécanisme international voisin d'exécution juridique ; selon de telles conditions d'alignement, l'exécutant sollicité peut reconnaître la valeur juridique d'une règle de droit ne lui étant pas associée et ainsi étendre son répertoire normatif (Cour EDH, 3^e sect., *Maire c. Portugal*, 26 juin 2003, n° 48206/99, §72, où la Cour EDH s'appuie sur la Convention de New York de 1989 pour résoudre le litige).

³⁸⁵CC, *M. Georges F. e. a.*, 23 sept. 2016, n° 2016-567/568 QPC : « 8. (...) les dispositions [litigieuses], qui méconnaissent l'article 2 de la Déclaration de 1789, doivent être déclarées contraire à la Constitution ; (...) 11. la remise en cause des actes de procédure pénale consécutifs à une mesure prise sur le fondement des dispositions déclarées contraires à la Constitution méconnaîtrait l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et aurait des conséquences manifestement excessives [on souligne]. Par suite, les mesures prises sur le fondement des dispositions déclarées contraires à la Constitution ne peuvent, dans le cadre de l'ensemble des procédures pénales qui leur sont consécutives, être contestées sur le fondement de cette inconstitutionnalité. »

règle perd son objet à s'appliquer au cas concret en qualité de norme constitutionnelle suprême. L'objet normatif de l'article 2 est tout simplement incompatible avec les circonstances du cas concret, de quoi il en découle l'inapplicabilité de cet objet en l'espèce.

La norme n'est toutefois pas la seule unité objective à laquelle peut être ramenée la règle de droit $F \rightarrow C$ dans le cadre d'une contradiction entre règles de droit. Ainsi que le recensent R. Guastini et V. Champeil-Desplats³⁸⁶, l'ancienneté de la règle (*lex posterior derogat priori*, hiérarchisation formelle selon la date de création de la règle), sa spécialisation (*lex specialis derogat generali*, hiérarchisation matérielle selon le niveau de détail de la règle) ou encore la vertu sociale/morale/politique qui lui est attribuée par l'exécutant (hiérarchisation axiologique selon un jugement de valeur porté sur la règle) représentent autant d'objets auxquels cette règle peut être rattachée afin de résoudre sa contradiction avec une autre règle. Au-delà même de ces situations de contradictions de règles, la règle de droit est rapportable à d'autres objets qui, à l'instar de l'objet normatif, peuvent se révéler incompatibles avec les circonstances de l'espèce et ainsi entraver l'application de cette règle dans le cas concret. Par exemple, l'accord franco-russe du 27 mai 1997 – par lequel la France a renoncé à protéger diplomatiquement ses ressortissants créanciers auprès du Trésor public russe d'emprunts contractés par la Russie avant 1917, moyennant quoi la Russie s'est engagée à verser à la France une somme d'argent pour indemniser lesdits créanciers – un tel accord est pourvu d'un objet exclusivement interétatique, n'engendrant donc aucun droit subjectif dont pourrait se prévaloir un créancier dans un contentieux contre l'État³⁸⁷. Ou encore, si la règle de droit a pour objet un « principe » constitutionnel, elle peut potentiellement lier le législateur, mais elle ne peut directement lier l'administration contre laquelle l'administré invoque ce principe³⁸⁸. Dans ces situations, l'objet de la règle (dont les caractéristiques retenues la ramènent à une unité normative, interétatique ou de principe constitutionnel) la rend incompatible avec le cas concret en présence (incompatibilité de l'objet « normatif » avec un contentieux mettant gravement en jeu l'ordre public, incompatibilité de l'objet « interétatique » avec un contentieux non-interétatique, incompatibilité de l'objet « principe constitutionnel » avec un contentieux excluant le législateur). La règle n'ayant pour objet de s'appliquer à ce cas, l'exécutant l'invalidera dans ce cas. Inversement, si la règle invoquée vaut prescription dans le cas concret (s'il y a alignement du mécanisme d'exécution associé à la règle et de l'exécutant sollicité), et si elle a pour objet de s'y appliquer (si son objet est compatible avec le cas concret), cette règle peut être validée par l'exécutant. Est ainsi levée la deuxième incertitude : la règle $F \rightarrow C$ trouve enfin concrétisation, *i.e.* validation dans un cas concret. Une fois reconnus la valeur de la règle dans le cas concret et son objet à s'y appliquer, la règle peut certes être tenue pour valide dans ce cas concret, mais la possibilité d'appliquer la règle à ce cas ne dépend pas seulement d'éléments afférents à la règle. Extérieure à cette règle, l'intervention factuelle survenue dans le cas concret doit à son tour être reconnue comme justifiant l'application de la règle pour que soit levée la troisième incertitude : la règle peut-elle s'appliquer au cas concret ?

Cette troisième incertitude est due à une correspondance *prétendue*, donc non encore *établie*, entre l'intervention factuelle et F. Ne sachant pas en effet si l'intervention factuelle

386GUASTINI Riccardo, *Leçons de théorie constitutionnelle*, préc., Dalloz, 2010, p. 75s. ;

CHAMPEIL-DESPLATS Véronique, « Hiérarchie des normes, principe justificatif de la suprématie de la constitution », in TROPER Michel et CHAGNOLLAUD Dominique (dir.), *Traité international de droit constitutionnel*, Tome 1, Dalloz, 2012, p. 733-763

387CE Ass., *M. Kandyrine de Brito Paiva*, 23 déc. 2011, n° 303678

388Par ex., CAA Bordeaux, 6^e ch., 14 oct. 2013, 12BX02069, inédit au recueil Lebon

correspond à F, on ignore si elle justifie l'application de C. Il incombe dès lors à l'exécutant d'établir (valider) ou au contraire de dénier (invalider) cette correspondance – ainsi revient-il au juge de dire si les « propos tenus » (intervention factuelle) sont des « discours haineux » (F) à l'occasion de la qualification juridique des faits. La validation porte donc non sur la règle prise comme « objet », comme unité indissociable $F \rightarrow C$, mais sur le « sujet »³⁸⁹ de la règle, à savoir la seule composante F de la règle $F \rightarrow C$. En d'autres termes, ce qui est validé ici n'est pas la règle elle-même mais le remplissement de F par l'intervention factuelle : si l'intervention factuelle correspond à F, F est rempli et justifie l'application de C. Il arrive encore que F soit rempli, puis vidé par l'application d'une autre règle. Pour ne donner que trois exemples de ces « autres règles », une renonciation à un droit³⁹⁰, une illégalité³⁹¹ ou encore une négligence³⁹² de la part de celui qui prétend une correspondance de l'intervention factuelle avec F auront pour effet de vider F (même rempli) de sa capacité à provoquer l'application de C³⁹³. Inversement, si la correspondance est établie sans être inhibée par de telles contre-règles, l'exécutant retiendra que cette validation de F dans le cas concret justifie l'application de C. Il sera alors en mesure d'ordonner l'application concrète de C, ouvrant par-là l'étape suivante.

5^e étape : l'application de la règle dans un cas concret. Seulement après qu'aient été levées toutes les incertitudes sur l'état prescriptif de la règle dans le cas concret, il devient possible de l'appliquer à ce cas. L'application renvoie ici à l'opération par laquelle est accomplie la conséquence C, par laquelle il lui est fournie une traduction dans le ressort du destinataire chargé de supporter C. On identifie donc l'applicateur comme la personne chargée de réaliser C sur ordre d'application : si la règle condamnant les discours haineux a été validée pour s'appliquer aux propos tenus dans un cas concret, l'applicateur pourrait être l'administration étatique (lorsque l'exécutant ordonne une amende), ou encore le FAI (lorsque l'exécutant ordonne le blocage du site/de la page sur lequel est hébergé le contenu haineux), l'hébergeur (lorsque l'exécutant ordonne la suppression du contenu haineux) etc. À l'issue de l'application, la prescription achève son processus de réalisation, depuis sa formation abstraite jusqu'à son accomplissement concret.

L'ensemble de ce processus peut être modélisé comme suit :

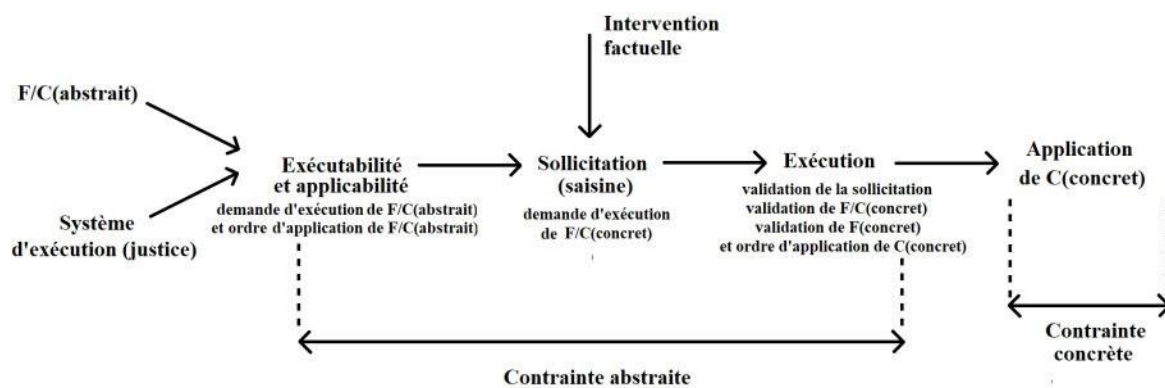
389On définira ici sommairement le « sujet » comme l'élément divis d'une unité à laquelle il est assujéti

390Par ex., en contentieux des droits de l'Homme : FRUMER Philippe, *La renonciation aux droits et libertés*, Bruylant, 2001

391Par ex., en droit pénal : le principe de loyauté de la preuve implique l'interdiction de provoquer la commission d'une infraction, en sorte que l'illicéité des méthodes pénales employées pour découvrir une infraction ne saurait engendrer la condamnation de cette infraction (par ex., Cass. crim., Cyril X, 4 juin 2008, n° 08-81.045)

392Par ex., en droit civil : v. les nombreuses applications de l'adage « Nul ne peut se prévaloir de sa propre turpitude »

393On note toutefois, pour chacune de ces situations, que F peut difficilement être vidé lorsque la règle a un objet « indérogeable », « d'ordre public » etc. Le sujet et l'objet de la règle peuvent donc tout à fait interagir dans le travail de validation effectué par l'exécutant. En d'autres termes, les trois incertitudes levées ne le sont pas nécessairement dans l'ordre de présentation ici exposé ; un tel agencement se veut pédagogique



Cette modélisation se veut « simple » en ce sens qu'elle entend retranscrire les étapes universellement suivies pour la concrétisation d'une prescription juridique, sans faire cas des diverses concrétisations possibles. Pour autant, si l'on a souhaité faciliter la compréhension de cette modélisation en éprouvant principalement la concrétisation d'une loi par le juge, on observera qu'une telle modélisation est valable pour d'autres prescriptions étatiques qu'une loi (circulaires, arrêtés préfectoraux, jurisprudence...), dans d'autres circonstances que celles d'une saisine du juge (publication d'une circulaire, communication d'un arrêté...).

En synthétisant la lecture de cette modélisation : lorsque la règle de droit est posée, le fait de conditionnement F , la conséquence prévue C et le rapport $F \rightarrow C$ constitutifs de cette règle sont dans un état abstrait, n'ayant encore rencontré aucun cas factuel dans lequel se concrétiser (1^{re} étape) ; si cette règle est associée à un mécanisme préexistant d'exécution et d'application tel un juge, alors elle comporte une exigence abstraite de conformité, *i.e.* une demande d'exécuter et un ordre d'appliquer la règle abstraite en-dehors de tout cas factuel (2^e étape) ; un cas concret ne commence à se former que par le croisement d'une intervention factuelle avec une sollicitation de l'exécutant, prétendant devant lui une correspondance de cette intervention avec le F de la règle abstraite et concrétisant ainsi la demande d'exécution abstraitement portée par la règle (3^e étape) ; appelé par cette demande concrète d'exécution, l'exécutant peut valider la sollicitation émise, l'état prescriptif de la règle invoquée et le remplissement des faits couverts par cette règle dans le cas concret, faisant ainsi entrer dans un état concret à la fois la règle abstraite et son F et concrétisant l'ordre abstraitement portée par la règle d'appliquer son C (4^e étape) ; sur cet ordre concret d'application, l'applicateur peut traduire la conséquence C dans le ressort (corporel, patrimonial, institutionnel...) de son destinataire, faisant ainsi entrer cette conséquence dans un état concret (5^e étape).

Une telle modélisation appelle plusieurs remarques. D'abord, le rôle de l'exécutant consiste d'une part à valider la règle dans le cas concret – nécessitant la triple validation dans le cas concret de la sollicitation, du caractère prescriptif de la règle et de son applicabilité – et d'autre part à formuler l'ordre concret d'appliquer la règle. L'exécutant est en ce sens celui qui donne le « feu vert » à l'applicateur pour que soit accomplie la conséquence C d'une règle.

Ensuite, chaque élément abstrait de définition d'une prescription trouve une traduction concrète : à travers ce processus, tant la règle (dans ses composantes F et C et dans son ensemble $F \rightarrow C$) que l'exigence de conformité (demande d'exécution et ordre d'application) deviennent concrets par la certitude de leur état antérieurement abstrait. Dès lors, les deux éléments retenus dans la définition substantielle de la prescription (une règle mise en support et une exigence de conformité) sont effectivement repris par ce processus, de la formation abstraite jusqu'à la réalisation concrète

de la prescription. La modélisation ici proposée confirme donc la définition substantielle de la prescription en qualité de règle exécutable et applicable (phase abstraite) dont l'accomplissement procède d'un ordre (phase concrète). Par cohérence avec ces résultats processuels et substantiels, et dans le cadre de cette thèse qui rapporte le Droit à l'État, on préférera pour la suite la formule plus adaptée de « **prescription étatique** » à celle de « prescription juridique », qu'on peut précisément définir comme **toute règle issue d'un créateur de droit habilité par l'État, exécutable et applicable par des exécutant et applicateur habilités par l'État, et dont l'accomplissement procède d'un ordre émis par cet exécutant.**

De plus, bien que les éléments abstraits se concrétisent progressivement tout au long du processus, on démêle clairement une **phase abstraite** et une **phase concrète** de la prescription étatique. La phase abstraite englobe les deux premières étapes (création de la règle, puis association de la règle à un mécanisme préexistant d'exécution et d'application) rassemblant tous les éléments prescriptifs exclusivement abstraits ($F, F \rightarrow C, C$, demande d'exécution et ordre d'application). En réunissant les éléments de définition d'une « prescription », la règle est abstraitement qualifiable comme telle à l'issue de cette phase. La phase concrète débute quant à elle lors de la troisième étape, au moment où se forme le cas concret : une règle ne peut être présentée à un exécutant dans une situation de fait que si une sollicitation (*i.e.* un appel déclencheur du mécanisme préexistant d'exécution) croise une intervention factuelle (*i.e.* tout fait dont est prétendue la correspondance avec le F de la règle abstraite). Ce croisement préalable est requis pour entraîner la validation par l'exécutant du remplissage de F dans le cas concret, et donc pour entraîner la conséquence C conditionnée par ce F . Fruit de ce croisement, le cas concret induit ainsi une rencontre de la règle avec les faits que couvre son F et fait se concrétiser un à un les éléments de la prescription abstraite jusqu'à l'application de la conséquence prévue C . On fait donc courir cette phase concrète d'une prescription étatique de la troisième à la cinquième étape.

Enfin, le destinataire de la règle (*i.e.* celui qui doit supporter la conséquence C) ne se la voit imposée qu'hypothétiquement de la deuxième à la quatrième étape incluse, sur le fondement de l'exigence abstraite de conformité attachée à la règle prescriptive. C'est seulement lors de l'ultime étape de l'application que le destinataire se la voit imposée physiquement, sur le fondement d'une exigence concrète de conformité. On dira de la prescription étatique que son effet contraignant est abstrait aussi longtemps qu'elle s'impose hypothétiquement dans le ressort du destinataire, et que cet effet contraignant se concrétise en appliquant effectivement la conséquence de la prescription dans le ressort du destinataire³⁹⁴.

Ainsi modélisée, cette propriété contraignante de la prescription nous fait à la fois confirmer et préciser notre définition de la prescription introduite dans l'annonce de ce premier chapitre, à savoir un « *ordre [de réaliser une règle, précisons-nous] dont l'existence contraignante persiste après l'édiction de cet ordre [confirmons-nous]* ». Cette définition « effective » de la prescription, axée sur les effets contraignants de l'ordre prescriptif, corrobore non seulement la définition substantielle qu'on en a dressée (« règle exécutable et applicable dont l'accomplissement procède d'un ordre ») mais aussi la définition processuelle ici détaillée (règle dont la réalisation résulte du suivi par cette règle des étapes d'un parcours prescriptif telles que retracées). Cette convergence des trois

³⁹⁴ Cette analyse nous ramène à notre théorie, exposée dans l'introduction, de la règle contraignante. On rappelle qu'on distingue deux types de contraintes posées par une règle : la contrainte abstraite (ou « pouvoir de contraindre », *i.e.* l'applicabilité systématique d'une conséquence C lorsqu'intervient le fait de conditionnement F) ; et la contrainte concrète (ou « contrainte effective », *i.e.* l'application concrète d'une conséquence C lorsqu'intervient le fait de conditionnement F).

définitions proposées quel que soit l'angle de vue depuis lequel on étudie la prescription (son effet contraignant, sa signification substantielle, son processus de réalisation) nous convainc que le concept de « prescription » tel qu'employé recouvre la même réalité pour chacun de ces emplois. Validé sous ces trois angles d'observations, ce concept nous apparaît suffisamment fiable pour en vérifier la présence dans un contexte numérique, et donc pour le mobiliser comme étalon de comparaison entre une règle de droit et une règle numérique.

B) Modélisation simple du processus prescriptif numérique

On rappelle qu'on réunit les instructions préalables (interruptions et exceptions) et les instructions machine sous le vocable de « règle machine », car ce sont les deux types d'instructions créées en langage machine. Pour modéliser le processus de réalisation emprunté par une règle machine, la question posée sera la même que pour la règle de droit, sans postuler que la règle machinale constitue une prescription. Quelles sont les étapes suivies par une règle issue du langage machine pour obtenir réalisation, pour obtenir une réaction machinale appliquant ladite règle ?

1^{ère} étape : la création d'une règle abstraite. Programmé dès la conception de la machine numérique, un langage machine corréle des suites binaires (composées de 0 et de 1) à des réactions machinales déterminées (réalisation d'opérations arithmétiques, comparatives, logiques ou de transfert). Chaque réaction machinale étant attribuable à la suite binaire qui lui est corrélée, on en déduit que cette corrélation a le caractère d'un rapport de conditionnement $F \rightarrow C$ où la réaction machinale C est conditionnée par la survenance de la suite binaire F. En posant ces corrélations, le langage machine pose ainsi des règles qui conditionnent une réaction machinale par une suite binaire mais qui, n'étant pas encore sollicitées dans un cas concret, demeurent à l'état abstrait.

2^e étape : l'association de la règle à une exigence abstraite de conformité. Seulement après avoir été posée, la règle créée par langage machine devient potentiellement réalisable. Comme pour la prescription étatique, cette potentialité est acquise par l'association de la règle-machine à un mécanisme d'exécution et d'application préexistant. Plus précisément, la préexistence d'un processeur est requise pour que puisse être réalisée une règle-machine. À nouveau, il n'est pas nécessaire que la règle soit effectivement exécutée et appliquée pour être réalisable ; il lui suffit pour cela d'être assortie d'une hypothèse d'exécution-application, *i.e.* de la possibilité d'être concrétisée par le processeur. On prend l'exemple de la règle préprogrammée dans la mémoire de la machine : <si 11100110 0010011 [instruction machine], alors le processeur doit récupérer les données d'adresse contenues dans la mémoire vive pour les transférer vers le registre SI du processeur>. Cette règle est associée à une hypothèse de mise en œuvre par un processeur et gagne de ce fait la potentialité d'être réalisée. Par l'acquisition de cette potentialité, la règle-machine porte génériquement, en-dehors de tout cas concret, une demande d'exécution et un ordre d'application, *i.e.* une exigence abstraite de conformité sur le fondement de laquelle elle pourra plus tard obtenir réalisation. En portant une telle exigence de conformité, la règle-machine quitte son état de simple règle : elle devient une prescription, une règle exécutable et applicable dont l'accomplissement procède d'un ordre.

3^e étape : la rencontre de la règle avec un cas concret. Seulement après que la règle est devenue exécutable et applicable, sa concrétisation peut être sollicitée en sa qualité de prescription. Comme pour la prescription étatique, cette sollicitation résulte d'une intervention factuelle extérieure à la règle qui prétend correspondre au F de ladite règle, appelant en conséquence la concrétisation de $F \rightarrow C$. Fort logiquement, la nécessité de l'intervention

factuelle s'explique là aussi par la structure même de $F \rightarrow C$: C étant conditionné par la survenance de F , la conséquence C (transfert des données d'adresse depuis la mémoire vive vers le registre SI) ne peut s'appliquer concrètement que si le fait F (11100110 0010011) est rempli par une intervention factuelle concrète (une production de données). En d'autres termes, l'utilisateur devra produire sur sa machine des signaux électriques qui correspondent exactement aux données 11100110 0010011 (F) pour qu'une adresse soit transférée vers SI et traitée par le processeur (C).

Par la structure même d'un rapport $F \rightarrow C$, il est donc nécessaire qu'une intervention factuelle surgisse, prétende correspondre à F pour appeler la concrétisation de $F \rightarrow C$. Aussi faut-il en déduire que la concrétisation d'une règle-machine est sollicitée par une correspondance *prétendue*, et non *établie*, entre une intervention factuelle et F . Cette sollicitation pour que soit concrétisée une règle-machine ne peut prendre qu'une seule et unique forme : celle d'une requête d'accès, découlant d'une correspondance prétendue de l'intervention factuelle (production de données) avec le F (11100110 0010011) prévu par la règle.

En pratique, supposons que le producteur de données veuille produire un message contenant la seule lettre R, et supposons que l'instruction qui ordonne l'exécution de la lettre R (« instruction R » ci-après) se situe dans la mémoire vive à l'adresse 00000101 00001101 : sa requête d'accès comportera la règle ordonnant le transfert depuis la mémoire vive vers SI (11100110 0010011) suivie de l'adresse à transférer, donc de l'adresse de l'instruction qui ordonne l'exécution de la lettre R (00000101 00001101). Dans notre exemple, pour ordonner au processeur de récupérer cette dernière instruction dans la mémoire, le producteur de données devra donc émettre la requête suivante 11100110 0010011 00000101 00001101.

Instruction machine d'adressage (règle ordonnant abstraitement l'exécution des données d'adresse par transfert de la mémoire vive vers ESI)	
11100110 0010011	

Requête d'accès à l'adresse de l'instruction R (règle ordonnant concrètement l'exécution de l'adresse où se situe l'instruction R)	
Opérateur de l'instruction machine (ordre de transférer l'adresse de la mémoire vive vers ESI)	Opérandes de l'instruction machine (adresse de l'instruction R)
11100110 0010011	00000010 00001101

Lorsque le processeur aura récupéré l'adresse de l'instruction R, il pourra exécuter cette dernière. À nouveau, l'instruction R est composée d'un opérateur qui prévoit les opérations à effectuer, et des opérandes qui mentionnent les données sur lesquelles effectuer les opérations. Supposons : que l'opérateur 10100000 ordonne au processeur d'ajouter dans le registre A les opérandes qui suivent et d'additionner ces opérandes (<si 10100000, alors ajout dans le registre des données contenues dans l'opérande et addition de ces données>) ; et que les données de caractère correspondant au début d'un message et à la lettre R s'écrivent 00000001 01010010.

Instruction machine d'incrémentation et d'addition (règle ordonnant abstraitement l'exécution des données par addition et par ajout des données dans le registre A)
10100000

Requête d'accès à l'insertion de la lettre R (règle ordonnant concrètement l'exécution d'un message débutant avec la lettre R par addition et ajout des données dans le registre A)	
Opérateur de l'instruction machine (ordre d'incrémenter et d'additionner les opérandes dans le registre A)	Opérandes de l'instruction machine (données de caractères correspondant à un texte débutant par la lettre R)
10100000	00000001 01010010

La « sollicitation » ici identifiée (requête d'accès) renvoie donc à la même signification que celle mobilisée pour décrire le processus de réalisation d'une prescription étatique, à savoir l'appel déclencheur d'un mécanisme préexistant d'exécution. Par ailleurs, cette sollicitation couvre les deux mêmes intérêts pour la réalisation d'une prescription numérique que ceux observés pour la réalisation d'une prescription étatique. D'une part, elle place la règle-machine abstraite (incrémentation et addition des opérandes dans le registre A si 10100000) devant un cas concret (par ex. l'enclenchement de la touche R du clavier), et appelle ainsi la concrétisation de cette règle. D'autre part, cette sollicitation convertit en *acte* (acte de production d'une requête d'accès) une demande d'exécution jusqu'alors *abstraitement* portée par la règle machine, et concrétise ainsi cette demande. À la différence notable de la plupart³⁹⁵ des prescriptions étatiques toutefois, on constate que la sollicitation couvre un troisième intérêt pour la réalisation d'une prescription numérique : l'acte de production d'une requête d'accès a pour effet de concrétiser non seulement la demande d'exécution, mais également l'ordre d'application. Cette différence s'explique par la concentration des fonctions d'exécution et d'application au sein d'un même exécutant-applicateur – le processeur. En raison de cette concentration exécution-application, l'ordre d'application qui précède nécessairement l'application peut par-là même précéder l'exécution. De cette façon, le processus prescriptif numérique rend possible l'antériorité de l'ordre d'application par rapport à l'exécution, en sorte que la requête d'accès concrétise un ordre d'application qui n'est pas formulé par l'exécutant mais issu de la sollicitation.

4^e étape : l'exécution et l'application de la règle dans un cas concret. Seulement après avoir été sollicitée par une demande d'exécution et d'application dans un cas concret, la règle peut être exécutée puis appliquée pour ce cas. Il est évidemment ici prêtée à l'« exécutant » la même définition que celle employée pour le processus prescriptif étatique, à savoir un validateur dont le rôle consiste à lever les incertitudes sur l'état prescriptif d'une règle (une règle machine si l'exécutant est numérique). Les incertitudes sont les trois mêmes que celles rencontrées avec la prescription étatique.

La première incertitude (la règle invoquée peut-elle être exécutée dans le cas concret ?) est due à une concrétisation *sollicitée* de la règle machine par la requête d'accès, donc non encore *obtenue*. Pour arrêter l'incertitude sur le sort de cette sollicitation, le processeur s'assure qu'il est sollicité

³⁹⁵On constatera *infra* que certaines PE peuvent être exécutées sans recourir à une conversion

par une requête d'accès valide, qu'il pourra alors exécuter à ce titre. La requête d'accès est valide si elle respecte les conditions techniques de sa formalisation. *A priori*, cela ressemble fort aux conditions de recevabilité d'une saisine pour l'exécution d'une prescription étatique. Toutefois, mise à part la confusion exécution-application déjà relevée, on remarque ici une autre différence avec la saisine : les conditions de validité de la requête d'accès sont exclusivement formelles, tandis que les conditions de validité d'une saisine sont en partie substantielles. Dans le cadre de la prescription étatique, le juge doit par exemple apprécier l'intérêt à agir du requérant ; dans le cadre d'une prescription numérique, **la validité d'une requête d'accès ne dépend d'aucune appréciation de la part du processeur**. Soit la requête d'accès est produite dans un format exécutable pour la machine numérique (format d'un datagramme IP, format d'une instruction machine...), et le processeur valide la requête ; soit elle est produite dans un format non exécutable pour la machine numérique, et alors le processeur est incapable de la valider. Ainsi, la validité de la requête n'est pas appréciée par le processeur : elle s'impose à lui.

La deuxième incertitude (la règle invoquée trouve-t-elle exécution dans le cas concret ?) interroge la validité, non de la sollicitation, mais de la règle dont l'exécution est sollicitée. Lorsque le processeur est appelé à exécuter une règle, deux options s'offrent à lui : soit la règle est cohérente avec les autres règles stockées par la machine, et le processeur la validera ; soit la règle est incohérente avec les autres règles stockées par la machine, et le processeur l'invalidera. L'incohérence survient en principe lorsque les règles posées par un logiciel ne respecte pas les autres règles déjà hébergées par la machine - une instruction logicielle qui combine des instructions machine sans respecter leur niveau de privilège dans la mémoire, une instruction stockée à une adresse inexistante, un opérateur d'instruction machine qui contient des erreurs, un datagramme qui ne respecte pas les formalités requises... Là encore, ce mode de validation/invalidation de la règle par cohérence ressemble beaucoup à la validation/invalidation d'une règle de droit par le juge, qui vérifie la cohérence entre les prescriptions étatiques. Mais à nouveau, une caractéristique fondamentale différencie l'exécution d'une prescription étatique et celle d'une prescription numérique : le juge vérifie la cohérence entre les règles de droit grâce à la compatibilité *littérale* de leurs significations respectives ; le processeur de la machine numérique vérifie la cohérence entre les règles machine grâce à la compatibilité *mathématique* de leurs bits respectifs. Ainsi, le processeur n'a aucune marge pour évaluer la validité ou l'invalidité d'une règle : **l'exécution machinale est neutre en ceci qu'elle ne peut insérer aucune signification**, ne peut apporter aucun biais linguistique **lors de sa validation ou invalidation de la règle**.

Du côté de l'exécutant de la prescription étatique, on a observé une absence de neutralité lors de l'exécution de la règle de droit, durant laquelle les décisions prises par l'exécutant orientent l'issue de la validation de la règle. On a ainsi noté que : (i) au moment d'évaluer si la règle de droit invoquée a valeur prescriptive, *i.e.* si le mécanisme d'exécution abstraitement associé à la règle invoquée est aligné sur l'exécutant sollicité, les conditions de cet alignement peuvent varier selon l'entendement de l'exécutant (p. ex. une règle de droit international dont l'alignement sur le mécanisme français d'exécution est reconnu par un juge et dénié par un autre) ; (ii) au moment d'évaluer si la règle a pour objet de s'appliquer au cas concret, la signification prêtée à cet objet peut à son tour varier selon l'entendement de l'exécutant (p. ex., une règle ayant pour objet un « principe constitutionnel » signifié par le juge).

Inversement, du côté de l'exécutant numérique, la validation de la sollicitation ne résulte pas d'une décision prise par l'exécutant mais d'une cohérence mathématique, dont la seule existence la plus neutre révèle la validité de cette sollicitation. On note ainsi que : (i) au moment d'évaluer si la règle machine invoquée a valeur prescriptive, l'alignement du mécanisme d'exécution abstraitement associé à la règle et de l'exécutant effectivement sollicité se déduit de la préprogrammation de cette règle et de sa cohérence mathématique avec les autres règles programmées ; (ii) au moment d'évaluer si la règle-machine invoquée a pour objet de s'appliquer au cas concret, la signification prêtée à cet objet par l'exécutant ne peut être que celle communiquée par la requête d'accès en l'espèce. La détermination de l'objet de la règle par la sollicitation ainsi combinée avec la préprogrammation de cette règle et sa cohérence mathématique, la valeur prescriptive d'une règle-machine dans le cas concret est reconnue sans que la machine ait à émettre de décision.

En raison de cette neutralité, aucune décision prise par la machine ne s'intercale entre la validation (elle-même neutre) de la sollicitation et la validation de la règle. **La validité de la règle machine dans un cas concret est comme « liée » par la validité de la sollicitation** : la première dépend de la seconde. Si la requête d'accès est valide, la règle machine dont elle demande l'exécution l'est concomitamment dans le cas concret. *A contrario*, la validité d'une règle de droit est déliée de la validité de la sollicitation, une sollicitation valide (par ex., une requête recevable) n'impliquant pas nécessairement la validité de la règle elle-même dans le cas concret.

La troisième incertitude (la règle peut-elle être appliquée dans le cas concret ?) est, comme pour la prescription étatique, due à une correspondance *prétendue*, donc non encore *établie*, entre l'intervention factuelle et F. Pour lever cette dernière incertitude sur l'état prescriptif de la règle-machine invoquée, il revient à l'exécutant numérique de s'assurer que les données binaires produites (intervention factuelle) sont identiques à la suite binaire (F, soit 10100000 00000001 01010010 dans notre exemple de l'instruction R) prévue par la règle machine. Une fois de plus, la neutralité de l'exécution numérique la distingue de l'exécution étatique.

D'un côté s'agissant de la règle de droit, lorsque l'intervention factuelle prend la forme d'une situation, le remplissement de F dans le cas concret résulte de la correspondance faite entre une *situation* (intervention factuelle : propos tenus, refus de paiement, dégradation d'un panneau de signalisation...) et des *mots* (F : « discours haineux », « violation d'un droit de créance », « infraction de petite voirie »...). En pareil scénario, l'intervention factuelle (situation) ne partage pas le format littéral du F de la règle (mots), et leur correspondance, à défaut de pouvoir être déduite de leur identité formelle, ne peut alors être établie que si l'exécutant convertit une situation en mots – *i.e.* s'il qualifie juridiquement les faits. Par essence même, l'écart formel inévitable entre l'intervention factuelle et F procure à cette conversion le choix de plusieurs correspondances possibles. Par exemple, la *situation* dans laquelle le design d'un site web détermine la présentation des annonces publicitaires (intervention factuelle) peut-elle correspondre à la *qualification* juridique d'un hébergeur (F) ? On a constaté qu'un exécutant étatique y a d'abord répondu par la négative en 2006 pour Google AdWords, car le design de ce service joue un rôle actif en déterminant la présentation des annonces, privant ainsi ledit service de la qualité d'hébergeur ; puis qu'un autre exécutant étatique y a ensuite répondu par la positive en 2013 pour le même service, dont le

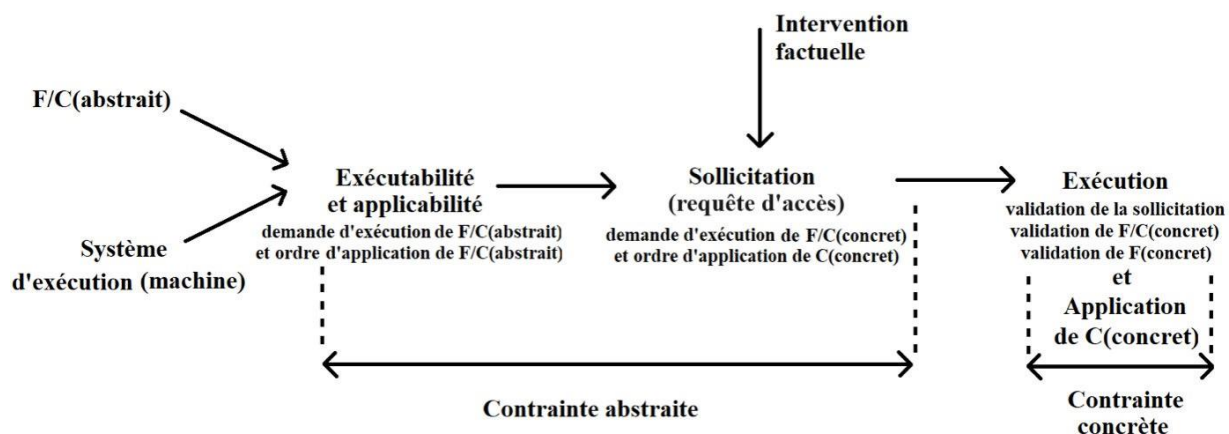
rôle inchangé du design a été jugé compatible avec la qualité d'hébergeur³⁹⁶. L'écart situation-mots laisse un espace : à une pluralité de correspondances possibles qui rend approximative la conversion « intervention factuelle → F » ; et à une évaluation des circonstances entourant le cas concret. Ainsi a-t-on relevé sur ce dernier point que les circonstances entourant le cas concret peuvent entraîner l'application de contre-règles qui inhibent la correspondance entre l'intervention factuelle et F, et qui vident un F *a priori* rempli.

De l'autre côté s'agissant de la règle machine, l'intervention factuelle prend *nécessairement* une forme chiffrée, et le remplissement de F dans le cas concret résulte alors de la correspondance faite entre une formule chiffrée (données binaires produites par l'intervention factuelle) et une autre formule chiffrée (bits incarnant le F de la règle stockée). L'intervention factuelle et F partageant un même format chiffré, leur identité formelle est alors possible, donc vérifiable, et leur correspondance peut être établie à l'identique sans opérer de conversion. En l'absence d'écart formel entre les chiffres produits par l'intervention factuelle et ceux visés par F, il n'est laissé de place ni à une pluralité de correspondances possibles, ni à une appréciation des circonstances entourant le cas concret. Faute d'un tel écart, la correspondance ne procède plus d'une approximation mais d'une exactitude excluant l'appréciation de l'exécutant. La validation de F dans le cas concret (son remplissement par l'intervention factuelle) ne peut résulter que d'une seule et unique correspondance (celle par laquelle les données binaires produites sont identiques à la suite binaire visée par F), et ne peut être inhibée par aucune contre-règle issue de l'appréciation des circonstances par l'exécutant. Tout comme l'exécutant numérique est incapable de prêter une signification à l'objet de la règle pour la valider, l'inexistence d'une conversion pour la validation de F dans le cas concret empêche cet exécutant de prêter une signification au sujet de la règle.

Les trois incertitudes sur l'état prescriptif de la règle machine invoquée dans le cas concret sont ainsi levées dans la plus grande neutralité de l'exécutant numérique, en ce sens qu'aucune décision prise par cet exécutant n'oriente la validation de la sollicitation, de la règle, ou de l'intervention factuelle conditionnant son application. L'application hérite de cette neutralité dans la mesure où elle se confond avec l'exécution : l'exécution de la règle (sa validation) par le processeur implique solidairement son application (la réalisation physique de C dans un cas concret) par le même processeur. Techniquement confondues, l'application ne peut diverger de l'exécution. Aucune décision de l'applicateur ne peut donc orienter la réalisation physique de C (réaction machinale) après qu'ait été validée la règle-machine dans le cas concret. Cette validité de la règle-machine dans le cas concret découlant elle-même de la validité de la sollicitation (requête d'accès), on confirme que l'ordre d'application concret d'une prescription numérique est formulé par la sollicitation et non par l'exécutant dont le travail de validation est neutre. À l'issue de son application, la prescription numérique achève son processus de réalisation.

On obtient la modélisation suivante :

396Respectivement CA Paris, 4^e ch. Sect. A, *Google France c. Louis Vuitton*, 28 juin 2006 ; CA Paris, Pôle 2 ch. 7, *Google Ireland, Google France c. Olivier M.*, 11 déc. 2013. On rappelle aussi qu'un autre exécutant encore y a répondu par la négative en 2017 pour un autre service, dont le rôle actif du design vis-à-vis de la présentation des annonces contribue à priver Alibaba de cette qualité TGI Paris, ord. 21 nov. 2017



Là encore, cette modélisation se veut « simple », elle entend retracer les étapes élémentairement et universellement suivies pour la concrétisation d'une règle-machine. En synthétisant la lecture de cette modélisation : lorsque la règle-machine est posée, le fait de conditionnement F , la conséquence prévue C et le rapport $F \rightarrow C$ constitutifs de cette règle sont dans un état abstrait, n'ayant encore rencontré aucun cas factuel dans lequel se concrétiser (1^{re} étape) ; si cette règle est associée à un processeur du fait de sa mémorisation par une machine numérique, alors elle comporte une exigence abstraite de conformité, *i.e.* une demande d'exécuter et un ordre d'appliquer la règle abstraite en-dehors de tout cas factuel (2^e étape) ; un cas concret ne commence à se former que par le croisement de l'intervention factuelle d'une production de données binaires avec la sollicitation du processeur, laquelle sollicitation concrétise à la fois la demande d'exécution et l'ordre d'application à travers une requête d'accès (3^e étape) ; le processeur ainsi sollicité en la double qualité d'exécutant-applicateur, il peut valider la requête d'accès émise par le producteur de données binaires, l'état prescriptif de la règle à exécuter et la correspondance de la règle machine mémorisée par l'ordinateur avec celle portée par la requête d'accès, de façon à traduire concrètement la conséquence C de cette règle dans le ressort physique de l'ordinateur destiné à supporter numériquement cette conséquence (4^e étape).

Une telle modélisation appelle plusieurs remarques. D'abord, l'ordre d'application ne résulte pas de l'exécution mais de la sollicitation pour les raisons déjà exposées. À la différence de la prescription étatique, ce n'est donc pas l'exécutant mais l'auteur de la sollicitation, à savoir le producteur de données binaires, qui accorde le « feu vert » à l'applicateur pour que soit accomplie la conséquence C d'une règle.

Ensuite, de même que le processus de réalisation d'une prescription étatique, celui d'une règle machine fait se concrétiser un à un chaque élément abstrait de notre définition de la prescription : tant la règle (dans ses composantes F et C et dans son ensemble $F \rightarrow C$) que l'exigence de conformité (demande d'exécution et ordre d'application) deviennent concrets par la certitude de leur état antérieurement abstrait. Dès lors, les deux éléments retenus dans la définition substantielle de la prescription (une règle mise en support et une exigence de conformité) sont effectivement repris par ce processus, de la formation abstraite jusqu'à la réalisation concrète de la prescription. Par cohérence avec ces résultats processuels et substantiels, on confirme que, de même que la règle de droit est constitutive d'une prescription étatique, **la règle-machine est constitutive d'une prescription « numérique »** (en raison de la nature de son processus de réalisation), dont on peut

confirmer la définition comme **toute règle issue d'un créateur de langage informatique, exécutable et applicable par une machine numérique, et dont l'accomplissement procède d'une requête d'accès émise par le producteur de données.**

De plus, à l'instar de la règle de droit, on note que la règle-machine commence par suivre une phase abstraite englobant les deux premières étapes du processus et tous les éléments abstraits de notre définition substantielle de la prescription (tant la règle dans ses composantes abstraites F et C et dans son ensemble $F \rightarrow C$, que l'exigence abstraite de conformité *via* les demande d'exécution et ordre d'application). Tout comme pour la règle de droit, la phase concrète de la règle machine est déclenchée à la troisième étape par le croisement de l'intervention factuelle (production de données binaires) avec la sollicitation de l'exécutant (requête d'accès). C'est à l'issue de ce croisement que peut germer un cas concret, dans le cadre duquel peut s'appliquer la conséquence C prévue par la règle machine lors de l'étape ultime clôturant la réalisation de cette règle. Dès lors, les moyens par lesquels une règle-machine trouve une existence abstraite et une existence concrète (création de la règle, association de la règle à un mécanisme d'exécution et d'application, intervention factuelle, sollicitation, exécution et application) sont similaires à ceux relevés pour une règle de droit en qualité de prescription étatique. Cette similarité processuelle finit de confirmer que **la règle de droit et la règle-machine sont comparables dans leur réalisation en tant que prescriptions.**

Enfin, semblablement à la prescription étatique, l'exigence de conformité abstraitement acquise par la règle machine dès la deuxième étape ne s'impose qu'hypothétiquement à l'ordinateur destinataire d'ici à ce que survienne la dernière étape (contrainte abstraite). Mais lors de cette dernière étape de l'application, à la différence de la prescription étatique qui ne s'impose physiquement à son destinataire qu'après son exécution, la règle machine s'impose dans le ressort physique de la machine destinataire immédiatement après la sollicitation (contrainte concrète). Par conséquent, contrairement à la contrainte concrète d'une prescription étatique qui inclut seulement son application, la contrainte concrète d'une règle machine inclut aussi bien son exécution que son application. On explique cette différence par la solidarité des fonctions d'exécution et d'application au sein du processeur : du fait de cette confusion exécution-application, l'ordre d'application nécessairement antérieur à l'application peut précéder l'exécution qui lui est appariée. L'exécution étant techniquement confondue avec l'application, l'ordre concret d'application nécessairement antérieur à l'application peut du même coup précéder l'exécution elle-même. Par cumul avec la neutralité de l'exécutant, cette confusion confie à la requête d'accès le rôle d'émettre l'ordre concret d'application antérieurement à l'exécution-application. Dès lors, **le pouvoir de faire se déployer concrètement l'effet contraignant d'une règle machine relève non de l'exécutant mais de l'auteur de la requête d'accès** (le producteur de données binaires)³⁹⁷.

On retire de cette comparaison de la règle de droit avec la règle machine que, comme la première, la seconde est constitutive d'une « prescription » sur des plans tant substantiel (la règle machine est une règle exécutable et applicable dont l'accomplissement procède d'un ordre) que processuel (les étapes élémentairement suivies par la règle machine pour se réaliser sont similaires à celles suivies par la règle de droit) ou même effectif (l'existence contraignante de l'ordre de réaliser une règle machine persiste après l'édition de cet ordre). Si la prescription numérique suit donc les mêmes processuelles que la prescription étatique, on a toutefois dénoté qu'elle ne les suivait pas de la même manière, que

³⁹⁷ Concernant les différents types de contrainte que l'être humain peut imposer à la machine numérique, on renvoie à l'Introduction dans laquelle on traite cette thématique

chacun de ces processus prescriptifs était doté de ses propres particularités pour assurer la réalisation ordonnée d'une règle. Ces marqueurs qui distinguent les deux processus étatique et numérique expriment pleinement leurs différences lorsque sont ciblées les relations prescriptives entre plusieurs règles de droit d'une part et les relations prescriptives entre plusieurs règles numériques d'autre part.

On définira les termes « requêtes d'accès à une donnée », « accès à une donnée » et « accessibilité d'une donnée » à partir de la modélisation proposée. On appellera ainsi « accessibilité d'une donnée » la possibilité de demander l'exécution et l'application d'une donnée ; on appellera « requête d'accès » la demande d'exécution et d'application d'une donnée (*i.e.* la sollicitation) ; on appellera « accès à une donnée » le stockage de cette donnée à l'issue de son exécution-application.

Chapitre 2. Le mode prescriptif numérique des données en ligne

On sait à présent que toute donnée binaire ne peut se réaliser qu'en empruntant des étapes proprement prescriptives. C'est toutefois dans les relations entretenues par les prescriptions numériques avec d'autres prescriptions numériques que leurs spécificités par rapport aux prescriptions étatiques deviennent manifestes (Section 1). L'approfondissement de ces spécificités nous permettra ensuite de les expérimenter pour constater que, malgré leur compréhension en qualité de « prescriptions » par la seule machine numérique, l'action et le pouvoir prescriptifs en ligne s'exportent dans les rapports de force inter humains (Section 2).

Section 1. Comparaison des relations inter-prescriptives étatiques et numériques

Durant son processus de réalisation, une prescription - PE ou PN - entre généralement en contact avec d'autres prescriptions de même catégorie - respectivement PE ou PN -, d'où l'on tire une modélisation « complexe » retranscrivant les particularités de la PE (Paragraphe 1) et de la PN (Paragraphe 2) dans leur propre contexte relationnel.

Paragraphe 1 – Modélisation complexe du processus prescriptif étatique

Lors de notre précédente comparaison des processus prescriptifs étatique et numérique, nous nous sommes bornés à une modélisation simple retraçant les étapes basiques suivies par ces prescriptions pour se réaliser. Une telle comparaison, destinée à vérifier le caractère prescriptif d'une règle machine, portait alors sur ces étapes bien plus que sur les prescriptions étatiques et numériques elles-mêmes. Leurs étapes de réalisation étant théoriquement universelles pour toute prescription telle que définie, elles n'offrent que rudimentairement de déceler les spécificités d'une prescription étatique par rapport à une prescription numérique et inversement. Comparer les spécificités de ces deux catégories de prescriptions appelle une modélisation plus complexe, décentrée de ces étapes universelles et recentrée sur le contexte prescriptif propre à chacune de ces catégories. Pour cerner ce contexte propre à une prescription étatique (PE), on scrutera la manière dont une telle prescription interfère avec d'autres PE dans son processus de réalisation. Les interférences examinées ici seront celles ayant cours durant la phase concrète d'une prescription étatique, soit à compter de la formation d'un cas concret par une intervention factuelle et une sollicitation. La même étude sera ensuite menée pour la prescription numérique (PN) afin de comparer leurs spécificités prescriptives concrètes.

S'agissant de la PE, on relèvera les interférences avec les autres PE qu'elle rencontre, depuis la naissance d'un cas concret jusqu'à l'accomplissement de cette PE. Pour en faciliter la compréhension, on suivra le parcours prescriptif de l'art. 8 de la Conv. EDH garantissant le droit au respect de la vie privée et familiale. Pour admettre cette convention *internationale* au nombre des prescriptions *étatiques*, on rappelle que notre utilisation de l'adjectif « étatique » couvre les prescriptions officiellement considérées par l'État comme dotées d'une valeur juridique, soit au terme de leur production par les pouvoirs constitutifs de l'État (par ex., législateur, juge et administration), soit au terme de leur production par des pouvoirs extérieurs que l'État habilite à créer de la valeur juridique (par ex., autorités fédérales, supranationales et internationales, autorités étrangères...). La Conv. EDH ne devant sa valeur juridique qu'à sa reconnaissance par au moins un État, on les tiendra elle et ses dispositions pour des prescriptions étatiques.

Retracer le parcours prescriptif de cet art. 8 oblige à remémorer sa phase abstraite, à savoir que : la règle contenue dans l'art. 8 (si une violation du droit à une vie familiale est imputable à un État (F), alors cet État doit faire cesser la violation (C)) a d'abord été posée par les auteurs de la Convention ; cette règle a ensuite acquis la qualité de prescription en étant associée à des mécanismes d'exécution (notamment la Cour EDH...) et d'application (les États). Dans le cadre de notre étude circonscrite à la phase concrète d'une prescription, c'est toutefois la suite du parcours de l'art. 8 qui nous intéresse.

Plaçons l'art. 8 face au cas concret suivant : des mineurs migrants se voient placés en rétention en même temps que leurs parents (intervention factuelle) ; à la suite de ce placement en rétention de « mineurs accompagnants », plusieurs de leurs parents demandent que soit exécutée dans le cas concret la règle prévue par l'art. 8 consacrant le droit à une vie familiale (sollicitation) ; la Cour EDH saisie à cette fin vérifiera la validité en l'espèce de la sollicitation exprimée (la requête est-elle recevable ?), de la règle (l'art. 8 a-t-il valeur juridique dans le cas concret et a-t-il pour objet de s'y appliquer ?) et du fait F qui en conditionne l'application (la rétention de mineurs accompagnants, *i.e.* l'intervention factuelle, correspond-elle à une violation du droit au respect de la vie familiale imputable à l'État, *i.e.* au F de la règle invoquée ?). On a constaté que, durant cette triple validation, le juge exécutant n'est pas neutre : incertain, l'état prescriptif de la règle dans le cas concret est orienté par les décisions de l'exécutant. Devant prendre des *décisions* pour résoudre ces incertitudes, le juge finit fatalement par prêter une nouvelle signification à la règle invoquée.

Pour l'illustration qui nous occupe, la Cour EDH vérifie la recevabilité de la requête en appréciant le respect par la sollicitation de ses conditions de recevabilité (intérêt à agir des requérants etc.), valide la règle dont l'exécution est requise (art. 8) en appréciant son objet (par ex. en qualité de norme issue de la Conv. EDH et des caractéristiques qui en découlent) et l'alignement de son mécanisme d'exécution (système de la Convention EDH) sur celui sollicité (Cour EDH), et déduit enfin son applicabilité au cas concret d'une conversion approximative (qualification juridique des faits) entre une situation (rétention de mineurs accompagnants) et des mots (violation du droit à la vie privée défini par l'art. 8). Chacune de ces appréciations amène la Cour EDH à *décider* le 19 janvier 2012³⁹⁸ que le placement de mineurs migrants accompagnants est contraire au droit au respect de la vie familiale consacré par l'article 8 de la Convention. La lettre de cet article 8 ne mentionne pourtant pas expressément l'inconventionnalité d'une législation autorisant la rétention des mineurs accompagnants. En prenant cette seule décision, le juge prête à l'article 8 une nouvelle signification, non inscrite dans la règle invoquée, qui tient la rétention de mineurs

398 Cour EDH, 19 janv. 2012, *Popov c. France*, n^{os} 39472/07 et 39474/07

accompagnants pour une violation du droit au respect de la vie familiale imputable à l'État. Se produit alors ce qu'on qualifiera de « **phénomène interprétatif humain** » consistant à **prêter une nouvelle signification par effet de médiation interhumaine**³⁹⁹.

En levant les incertitudes pour décider de l'état prescriptif d'une règle de droit dans un cas concret, l'exécutant prête donc une nouvelle signification à cette règle et, par interprétation, crée ainsi une nouvelle règle (*i.e.* une règle dotée d'une signification autre que celle interprétée). Dans notre illustration avec la Cour EDH, résoudre l'incertitude « *la règle $F \rightarrow C$ (si une violation du droit à une vie familiale est imputable à un État, alors cet État doit faire cesser la violation) peut-elle être validée et appliquée au cas concret (saisine de la Cour EDH à l'issue d'une rétention de mineurs migrants accompagnants) ?* » conduit la Cour à créer la règle « *si un mineur migrant accompagnant est placé en rétention (F), alors l'État doit faire cesser cette violation du droit au respect de la vie familiale (C)* ». Cette nouvelle règle forgée par l'interprétation de la Cour EDH a par ailleurs deux autres particularités : elle est associée à un mécanisme d'exécution (l'État partie à la Convention est garant de la validation de cette règle dans son ordre juridique interne) et à un mécanisme d'application (le même État est garant de la traduction physique de C auprès du destinataire de la règle, à savoir l'État lui-même). Exécutable et applicable, la règle émise par la Cour EDH est constitutive d'une prescription. Durant son parcours prescriptif pour se réaliser, l'art. 8 (prescription étatique PE-1) interfère donc avec une autre PE issue de l'interprétation faite par la Cour (prescription étatique PE-2). En d'autres termes, **par phénomène interprétatif, la prescription dont l'exécution est demandée change de PE-1** (l'État doit faire cesser toute violation du droit au respect de la vie familiale qui lui est imputable) **en PE-2** (l'État doit faire cesser les rétentions de mineurs accompagnants).

Surgit alors une nouvelle demande d'exécution, une nouvelle sollicitation pour que soit exécutée non plus PE-1 mais PE-2. Cette sollicitation peut prendre la forme d'une saisine du juge étatique, alors appelé à reconnaître la validité de PE-2 dans l'ordre juridique interne. Pour cette exécution de PE-2, on s'intéressera toutefois à une autre forme de sollicitation que la saisine du juge, la validation d'une PE par le juge ayant déjà été illustrée avec l'exécution de PE-1 par la Cour EDH. Rappelons que, portant une « demande d'exécution », la « sollicitation » désigne l'appel déclencheur d'un mécanisme préexistant d'exécution. La sollicitation ainsi entendue, le mécanisme d'exécution (l'État ici) peut être déclenché par divers types d'appels, tels que la saisine (du juge, d'une administration...) ou encore le dispositif d'un arrêt de justice⁴⁰⁰. C'est cette autre forme de sollicitation qu'on retiendra pour illustrer l'exécution de PE-2 : avant même qu'un juge interne soit saisi, le dispositif de l'arrêt rendu en l'espèce par la Cour EDH

399La décomposition étymologique du mot « interprétation » semble discutée. Le philologue Ernst Robert Curtius y voit les composantes *inter* (entre) et *pret* (connaître) comme si la connaissance humaine s'intercalait entre une chose et son interprétation humaine, tandis que le linguiste Michel Bréal estime que le radical impliqué dans *interpréter* n'est pas *pret* (connaissance) mais *pre* (prix) comme si l'interprétation désignait un échange voire un courtage dans un cadre linguistique de négoce : sur ces hésitations, v. dict. Littré, Entrée « Interpréter » [en ligne]. Le dictionnaire Gaffiot confirme qu'*interpretum* renvoie au « *bénéfice de courtage* » bien qu'*interpretor* renvoie à l'action d'« *expliquer, éclaircir* » ou à celle de « *servir d'interprète à la mémoire de quelqu'un* ». On s'en tiendra pour notre part à l'approche augustinienne, abordant l'interprétation comme des « *médiations humaines de la connaissance* » renvoyant à « *la relation (inter) de mutuel endettement (pretare), à l'état d'être proche (praesto) et à celui d'être présent (praesto esse)* » : THÉRIAULT Patrick, « *Per hominibus* : charité et herméneutique dans le prologue du *De doctrina christiana* », *Érudit*, vol. 62 (n°2), 2006, p. 369-380

400En principe doté de l'autorité de chose jugée, le dispositif d'un arrêt en synthétise la solution

demande à l'État de reconnaître la validité de la règle interdisant le placement en rétention de mineurs accompagnants. Via le dispositif de son arrêt, la Cour EDH sollicite ainsi l'exécution de PE-2 par cet État.

L'État a répondu à cette sollicitation par l'adoption d'une circulaire le 6 juillet 2012⁴⁰¹. Par l'adoption de cette circulaire, l'exécutant de PE-2 (le gouvernement ici) s'adonne au même travail que le juge pour la validation d'une prescription étatique, et doit donc lever les mêmes incertitudes sur l'état prescriptif de PE-2. À savoir : la règle PE-2 dont l'exécution est demandée peut-elle être exécutée dans le cas concret (la sollicitation, *i.e.* le dispositif de l'arrêt de la Cour EDH, est-elle valide dans l'ordre juridique interne) ? Cette règle trouve-t-elle exécution dans le cas concret (PE-2 est-elle valide dans l'ordre juridique interne) ? Et peut-elle être appliquée dans le cas concret (le F de PE-2 est-il valide en l'espèce par correspondance avec l'intervention factuelle) ?

Cette troisième incertitude invite à des précisions car, si l'on connaît ce en quoi consistent l'exécutant de PE-2 (gouvernement) et l'appel qui le sollicite (dispositif de l'arrêt de la Cour EDH), on ignore encore la consistance de l'intervention factuelle dans le cas concret.

	PE-1	PE-2
F	(si) Violation du droit à une vie familiale	(si) Rétention de mineurs accompagnants
C	(alors) Devoir pour l'État de faire cesser la violation	(alors) Devoir pour l'État de faire cesser les rétentions
Intervention factuelle survenue	Placement en rétention de mineurs accompagnants	???
Sollicitation	Saisine du juge	Dispositif de l'arrêt de la Cour EDH
Exécutant	Cour EDH	Gouvernement

Pour résoudre cette inconnue, on recherchera l'élément qui satisfait les deux fonctions caractéristiques d'une intervention factuelle dans un processus prescriptif. D'une part, on sait que, pour valider le F d'une prescription, ce F doit correspondre avec l'intervention factuelle qui engendre l'exécution. En partant d'un F déjà validé, il est donc possible de détecter l'intervention factuelle si l'on répond à la question : quelle est la correspondance grâce à laquelle F est validé ? S'agissant de PE-1 (art. 8, inconvictionnalité d'une violation du droit à une vie

⁴⁰¹On note que cette circulaire a été précédée d'une décision de Défenseur des droits n° MDE-2012-92 du 24 août 2012 relative au placement au centre de rétention administrative par décision de la préfecture d'une famille de nationalité angolaise, par laquelle l'autorité constitutionnelle indépendante appelle le ministère de l'Intérieur à exécuter l'arrêt *Popov* et à rechercher des solutions alternatives à la rétention d'une famille dont les parents migrants sont accompagnés de leurs enfants migrants. Pour autant, une telle décision du Défenseur des droits n'est pas constitutive d'une prescription, la règle qu'il propose n'étant pas appliquée à l'issue d'un ordre contraignant, *i.e.* d'un ordre qui s'imposerait dans le ressort du destinataire étatique. La règle ainsi créée par le Défenseur (si une famille de parents migrants est accompagnée d'enfants mineurs, alors doivent être appliquées des solutions alternatives à la rétention) est au mieux une règle recommandée et non une règle prescrite. À l'instar du dispositif de l'arrêt *Popov*, la décision du Défenseur peut donc être considérée comme une sollicitation du gouvernement pour l'exécution de PE-2 ; mais contrairement à l'arrêt *Popov*, la sollicitation émise par le Défenseur ne provient pas d'une prescription, et on ne la fera donc pas figurer dans la modélisation complexe d'un parcours prescriptif, qui se borne à retranscrire les relations inter-prescriptives nouées en l'espèce par l'art. 8 avec d'autres prescriptions étatiques d'ici sa réalisation.

familiale), son exécutant (Cour EDH) a reconnu le remplissement du F de PE-1 (violation du droit à une vie familiale) parce que, dans le cas concret, ce F correspond avec une rétention de mineurs accompagnants. Par conséquent, la survenance d'une telle rétention (*i.e.* le placement en rétention effectué) fournit le fait auquel correspond F pour être validé dans le cas concret. Le placement en rétention constitue donc l'intervention factuelle survenue pour conclure à la validation du F de PE-1. S'agissant de PE-2 (arrêt de la Cour EDH, inconvencionnalité de la rétention de mineurs accompagnants), son exécutant (gouvernement) a reconnu le remplissement du F de PE-2 (rétention de mineurs accompagnants) parce que, dans le cas concret, ce F correspond avec le contenu rédactionnel d'une circulaire. Par conséquent, la survenance d'une telle circulaire (*i.e.* la publication de la circulaire) fournit l'élément de correspondance grâce auquel F est validé dans le cas concret. La publication d'une circulaire constitue donc l'intervention factuelle survenue pour conclure à la validation du F de PE-2.

D'autre part, en plus de fournir le fait auquel doit correspondre F pour être valide dans le cas concret, on sait que l'intervention factuelle doit croiser une sollicitation pour que soit suscitée une exécution. En partant de la sollicitation de l'exécutant, il est donc possible de confirmer l'intervention factuelle identifiée si l'on répond à la question : cette sollicitation a-t-elle dû être croisée par l'intervention factuelle identifiée afin de susciter l'exécution d'une prescription ? S'agissant de PE-1, la saisine de la Cour EDH (sollicitation) dut effectivement croiser un placement en rétention de mineurs accompagnants afin que puisse être exécutée PE-1 dans le cas concret ; on peut donc confirmer que le placement en rétention de mineurs accompagnants incarne la survenance de l'intervention factuelle dont le croisement avec la sollicitation suscite l'exécution de PE-1. S'agissant de PE-2, le dispositif de l'arrêt de la Cour EDH (sollicitation) dut effectivement croiser la publication d'une circulaire afin que puisse être exécutée PE-2 dans le cas concret ; on peut donc confirmer que la publication d'une circulaire incarne la survenance de l'intervention factuelle dont le croisement avec la sollicitation suscite l'exécution de PE-2.

La validation de PE-1 et celle de PE-2 présentent toutefois une différence majeure : autant l'exécutant de PE-1 (Cour EDH) n'a pas produit l'intervention factuelle (placement en rétention) qui induit sa sollicitation ; autant l'exécutant de PE-2 (gouvernement) est cumulativement l'auteur de l'intervention factuelle (publication du contenu de la circulaire). De ce cumul exécutant-auteur de l'intervention factuelle, il en découle d'une part que cette intervention et la validation de PE-2 sont concomitantes : PE-2 devient valide dans l'ordre juridique interne en même temps qu'est publiée la circulaire. D'autre part, à la fois exécutant et auteur de l'intervention factuelle, le gouvernement forme lui-même le cas concret dans le cadre duquel il exécute PE-2 et valide sa propre intervention factuelle au moment de vérifier le remplissement de F dans ce cas concret. Déduite du remplissement de F par l'intervention factuelle, l'applicabilité de la règle dans le cas concret résulte alors de la décision de l'exécutant de former ce cas. En conséquence, pour que soit définitivement validée PE-2 et levée la troisième incertitude (PE-2 peut-elle être appliquée dans le cas concret ?), il suffit donc au gouvernement – agissant en qualité d'intervenant factuel – de publier une circulaire et – agissant en qualité d'exécutant – d'y inscrire le F de PE-2 (rétention de mineurs accompagnants), validant par-là sa correspondance avec l'intervention factuelle (contenu publié de la circulaire). De cette façon, à l'issue de son exécution de PE-2, le gouvernement reconnaît-il la possibilité d'appliquer PE-2 (arrêt de la Cour EDH prescrivant cessation des rétentions de mineurs accompagnants) dans l'ordre juridique interne.

Par cette exécution, le gouvernement crée-t-il une nouvelle prescription, comme l'a fait la Cour EDH vis-à-vis de l'art. 8 ? Théoriquement, le phénomène interprétatif pourrait être neutralisé par le format de l'intervention factuelle (circulaire publiée) requise pour la validation de PE-2. En effet, l'intervention factuelle n'a plus pour format une situation comme c'était le cas de l'intervention factuelle de PE-1, mais une rédaction, exactement comme PE-2 (l'arrêt de la Cour EDH étant écrit). L'intervention factuelle et le F de PE-2 partageant le même format, leur correspondance par l'exécutant ne nécessite pas de conversion et pourrait être identique : le gouvernement pourrait inscrire dans la circulaire la lettre même de PE-2, établissant ainsi une correspondance parfaitement identique entre la suite de mots composant l'intervention factuelle (circulaire) et celle composant la solution de la Cour EDH. Si la circulaire est un fac-similé de PE-2, aucun phénomène interprétatif ne se manifesterait puisqu'aucune nouvelle signification ne lui sera prêtée. Cependant, en l'espèce, le gouvernement n'a pas fait ce choix. Pour valider PE-2 dans l'ordre juridique interne, il a employé d'autres mots que ceux mobilisés par la Cour EDH. Dans sa circulaire, il demande aux préfets de région et de département et au préfet de Police de Paris de privilégier la procédure d'assignation à résidence plutôt que le placement en rétention « *dans le cas de familles parentes d'enfants mineurs* », exceptées trois situations pour lesquelles le placement en rétention est maintenu – le non-respect de l'assignation à résidence par la personne assignée, la fuite de l'un des membres de la famille et le refus d'embarquement. Ce faisant, à travers son exécution de PE-2, il lui prête une nouvelle signification, par ailleurs constitutive d'une nouvelle règle (si les parents migrants sont accompagnés de leurs enfants mineurs et hors les trois exceptions (F), alors l'assignation à résidence doit être privilégiée par rapport au placement en rétention (C)), par ailleurs associée à un mécanisme préexistant d'exécution et d'application (préfets). Au terme de sa validation de PE-2, le gouvernement opère donc ici une interprétation pour forger une nouvelle prescription PE-3, dont il sollicite l'exécution auprès des préfets en les désignant destinataires de la circulaire.

À leur tour, pour valider PE-3, les préfets devront lever les trois incertitudes pesant sur son état prescriptif : PE-3 peut-elle être exécutée dans le cas concret (la sollicitation, i.e. la désignation par la circulaire de ses destinataires, est-elle valide) ? Trouve-t-elle exécution dans le cas concret (PE-3 est-elle valide dans un cadre préfectoral) ? Peut-elle être appliquée dans le cas concret (le F de PE-3 est-il valide en l'espèce par correspondance avec l'intervention factuelle) ? Cette dernière intervention factuelle consiste ici dans la communication par laquelle le préfet ordonne l'application de la règle aux officiers et agents de police placés sous son autorité : c'est par correspondance avec cette communication qu'est validé le F de PE-3 (familles migrantes parentes d'enfants mineurs hors les trois exceptions de circonstances), et c'est par croisement avec cette communication que la sollicitation (désignation des préfets comme destinataires de la circulaire) peut susciter l'exécution de PE-

3. Comme on l'avait remarqué avec le gouvernement exécutant de PE-2, le préfet exécutant de PE-3 est ici aussi l'auteur de l'intervention factuelle et les mêmes conclusions peuvent en être tirées (l'intervention factuelle incarnée par la communication préfectorale et la validation de PE-3 sont concomitantes, et l'applicabilité de la règle dans le cas concret résulte de la décision du préfet de former ce cas). En principe exclusivement composée de mots, cette intervention factuelle (communication préfectorale) partage le même format littéral que le F de PE-3 (la circulaire PE-3 ayant la forme d'une rédaction), et leur correspondance pourrait alors être établie à l'identique si le préfet se bornait à reprendre la lettre de la circulaire dans sa communication, neutralisant ainsi le phénomène interprétatif. Au contraire, si le préfet employait d'autres mots que ceux mobilisés par la circulaire, même pour en préciser les termes, il lui prêterait une nouvelle signification, ferait œuvre d'interprétation, et forgerait une nouvelle règle (en remplaçant le F de PE-3 par un autre F) dont

il ordonne l'application auprès des mécanismes préexistants d'exécution et d'application (officiers et agents de police) y associés. On supposera ici que la communication préfectorale s'en tient à relayer littéralement la circulaire, de telle façon qu'aucune nouvelle règle n'est créée par interprétation préfectorale. Il n'en demeure pas moins que, par sa communication, le préfet ordonne aux officiers et agents de police l'application de la circulaire.

Enfin, les officiers et agents de police accomplissent la prescription PE-3 qu'il leur a été ordonné d'appliquer. Pour la première fois depuis le début de son parcours prescriptif, PE-1 (art. 8 Conv. EDH) trouve un accomplissement, c'est-à-dire que sa conséquence C (l'État doit faire cesser la violation qui lui est imputable du droit à une vie familiale) trouve une traduction dans le ressort (institutionnel ici) du destinataire de PE-1 (l'État, qui agit institutionnellement pour faire cesser ladite violation dans un cas concret). Or, durant ce parcours jusqu'à son accomplissement, PE-1 est devenu PE-3 par phénomène interprétatif en sorte que, pour l'applicateur de l'article 8 en l'espèce (officier/agent de police), PE-3 tient lieu de PE-1. On souligne néanmoins que, lors de son examen de PE-3, dont l'application lui a été ordonnée, l'applicateur se livre lui aussi à un travail de validation à l'issue duquel il peut invalider PE-3, *i.e.* en rejeter l'application dans le cas concret. Par-là, il se fait exécutant de PE-3 et doit lever les trois incertitudes pesant classiquement sur cette prescription dans le cas concret. PE-3 peut-elle être exécutée dans ce cas concret (l'ordre d'application qui sollicite l'applicateur est-il valide) ? Y trouve-t-elle exécution (PE-3 est-elle valide dans le cadre des missions de l'applicateur) ? Peut-elle y être appliquée (le F de PE-3 est-il valide en l'espèce par correspondance avec l'intervention factuelle) ?

Sur cette dernière incertitude, l'intervention factuelle consiste ici dans l'action par laquelle l'applicateur met en œuvre PE-3 : c'est par correspondance avec cette action qu'est validé le F de PE-3 (familles migrantes parentes d'enfants mineurs selon les modalités fixées par le préfet), et c'est par croisement avec cette action que l'ordre d'application émis par le préfet peut susciter l'exécution de PE-3. Une fois de plus, l'applicateur exécutant de PE-3 est par ailleurs l'auteur de l'intervention factuelle et les mêmes conclusions peuvent en être tirées (l'intervention factuelle incarnée par l'action policière et la validation de PE-3 sont concomitantes, et l'applicabilité de la règle dans le cas concret résulte de la décision de l'officier/agent de former ce cas). Partant, l'applicateur qui refuse de procéder à un acte d'application ne fournit pas l'intervention factuelle requise pour établir cette correspondance, et invalide du même coup le F de PE-3 dans le cas concret⁴⁰².

⁴⁰²Les illustrations d'une telle invalidation sont nombreuses : en 2018 par ex., plusieurs universitaires ont refusé d'appliquer la sélection algorithmique de Parcoursup prescrite par la loi n° 2018-166 du 8 mars 2018 relative à l'orientation et à la réussite des étudiants. Ou plus récemment, comme l'a révélé un courrier adressé le 26 janvier 2021 à la Direction générale de l'offre de soins (Jérôme Salomon) par le Syndicat national des biologistes des hôpitaux (SNBH) et publié sur Twitter par le même syndicat, la Direction générale de la santé a émis le 23 janvier un DGS-urgent (message d'alerte destiné aux professionnels de santé) n°8 en continuité du DGS-urgent n°5 sur la stratégie de freinage de la propagation des variantes du SARS-COV2 qui, par exécution d'un arrêté ministériel réservant au laboratoire Eurofins Biomnis l'agrément pour fabriquer des kits de criblage de variantes (notamment britanniques), impose de fait aux biologistes de réaliser une deuxième RT-PCR avec ce kit. Ainsi que le dénonce le biologiste @BioHospitalix (apportant pourtant régulièrement son soutien au gouvernement) sur son compte Twitter le 26 janvier 2021 : « *je suis dans une colère noire contre le ministère [de la santé] et les Ars. Ils nous interdisent de cribler les variants anglais avec une technique que l'on avait tous. Ils donnent le monopole de cette analyse à [Eurofin Biomnis] pour l'instant. L'intégralité des laboratoires de virologie est en train de se rebeller sur ce truc débile. On ne suivra pas l'arrêté. Et d'ailleurs tenez vous bien l'ARS Île de France nous demande de ne pas*

Cette exécution par l'applicateur est-elle créatrice d'une nouvelle prescription ? On note ici que le format de l'intervention factuelle (action de l'applicateur) n'est pas partagé par le F de PE-3 (la circulaire ayant un format littéral). Leur correspondance requiert donc que des mots soient convertis en action. L'écart entre les deux formats laisse un espace dans lequel s'insère inévitablement un spectre de différences entre les mots et l'action, allant de différences infimes à des différences majeures vis-à-vis de PE-3. Le comportement de l'agent qui applique PE-3 (l'intimidation ou la sérénité dégagés par l'agent, le ton et les mots employés pour s'adresser aux parents/enfants, les gestes pratiqués...) distingue nécessairement ce comportement de la lettre de PE-3, rendant impossible une correspondance parfaitement identique entre l'intervention factuelle et le F de PE-3. Le phénomène interprétatif ne pouvant alors être neutralisé, une nouvelle signification comportementale est prêtée à PE-3 par l'applicateur qui forge ainsi une nouvelle règle (par ex., si les parents migrants sont accompagnés de leurs enfants mineurs selon les modalités fixées par la circulaire (F), alors l'applicateur doit adopter un comportement serein pour privilégier l'assignation à résidence sur le placement en rétention (C)). Rétroactivement associée à un mécanisme préexistant d'application (officiers et agents de police) qui en permet la réalisation, cette règle porte les traits d'une prescription PE-4. **In fine, la conséquence C prévue par PE-4 peut ainsi être regardée comme l'une des (innombrables) réalisations de PE-1** (art. 8 Conv. EDH).

Pour la conséquence C de la prescription PE-1 (cessation d'une violation du droit à la vie familiale imputable à l'État), c'est donc finalement la conséquence C de la prescription PE-4 (comportement policier serein privilégiant l'assignation à résidence sur le placement en rétention) qui obtiendra une réalisation dans le ressort du destinataire de PE-1 *via* l'action policière. Au terme d'une chaîne de validations par interprétation, le C de PE-4 dévie du C de PE-1 par approximation des significations successives : l'application du C de PE-4 peut ne pas permettre la réalisation du C de PE-1 (un comportement policier serein *privilégiant* l'assignation à résidence *sans exclure* toute hypothèse de rétention de mineurs accompagnants peut ne pas suffire à faire cesser une violation du droit à la vie familiale au sens de l'art. 8 Conv. EDH) ; et le C de PE-1 peut trouver d'autres applications que celle proposée par le C de PE-4 (la cessation d'une violation du droit à la vie familiale peut trouver d'autres réalisations physiques qu'un comportement policier serein privilégiant l'assignation à résidence sur le placement en rétention de familles migrantes parentes de mineurs).

En somme, **par phénomène interprétatif, l'accomplissement de PE-1** (art. 8 Conv. EDH) **dans le cas concret** (application policière limitant le placement en rétention de mineurs migrants accompagnants) **se traduit par la réalisation de PE-4**. Les interprétations interférant dans le parcours prescriptif de PE-1 ne sont toutefois pas totalement libres : chacune résulte d'une validation qui, elle-même, nécessite d'établir une correspondance de l'intervention factuelle avec le F de la prescription à exécuter. Une prescription PE-2 créée par interprétation d'une prescription PE-1 ne pouvant l'être qu'en correspondant au F de PE-1, le F de PE-2 est nécessairement plus ou moins semblable au F de PE-1. Même entrecoupée par l'interprétation, **la chaîne prescriptive reliant PE-1 à PE-4 suit donc un cadre factuel à peu près stable** grâce auquel, de validation en validation, le F de PE-4 réalisée ne discordé en principe pas totalement avec le F de PE-1 édictée⁴⁰³. Rapportable à des origines processuelles (qui

suivre l'arrêté. ». L'inaction de l'applicateur entraîne l'invalidation, par cet applicateur dans le cas concret, de la prescription qu'il lui a été ordonné d'appliquer.

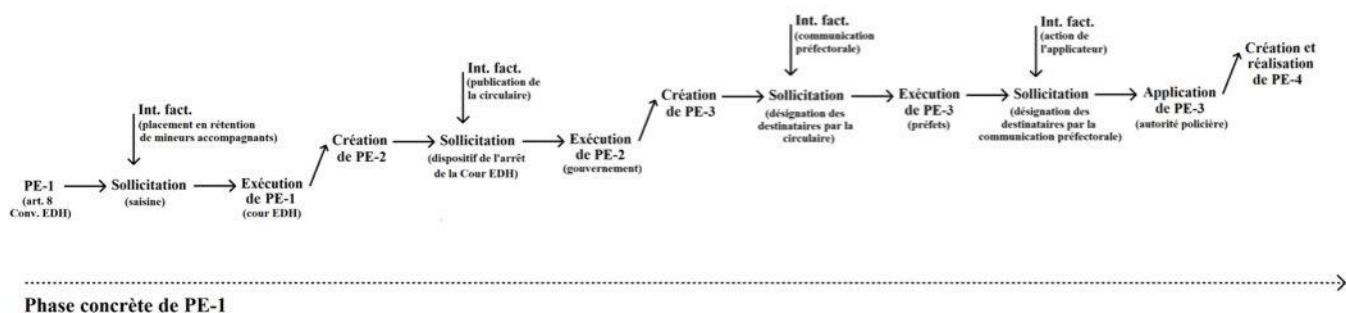
403En principe, le risque d'une discordance excessive entre le F de PE-1 et celui de PE-4 est entravé *en amont* par la structure même de ce processus. Un écart trop important entre l'intervention factuelle et le F de la prescription à exécuter empêcherait en effet l'établissement de leur correspondance par

requièrent une correspondance établie avec le F de la règle à exécuter pour la valider), cette stabilité reliant les F des prescriptions successives nous semble pouvoir expliquer en partie la **relative cohérence entre des prescriptions étatiques issues d'interprétations souveraines**. En complément de l'explication proposée par M. Troper d'une interprétation juridique stabilisée par un « système » de jeu analogue aux échecs (v. Introduction), on observe ainsi que l'interprétation étatique est par ailleurs stabilisée par le processus même suivi par les prescriptions étatiques afin de se réaliser comme telles⁴⁰⁴. Par la cohérence approximative entre les prescriptions formées par les exécutants et applicateurs jusqu'à l'accomplissement de PE-1, **cette stabilité du cadre factuel garantit à PE-1 une effectivité minimale inhérente au processus prescriptif étatique**, en ce sens que la correspondance requise avec le F de la règle exécutée réduit les risques que les faits *in fine* couverts par PE-4 contredisent ceux initialement couverts par PE-1.

On aboutit à la modélisation complexe :

l'exécutant, invalidant ainsi la règle avant qu'elle puisse atteindre l'étape de son application et donc la formation de PE-4. Dès lors, une prescription étatique ne peut obtenir de réalisation que si le F de la prescription à réaliser PE-1 concorde suffisamment avec le F de la prescription réalisée PE-4. Pour mobiliser un exemple déjà vu, en considérant que des perquisitions menées sur le fondement d'une loi inconstitutionnelle ne peuvent être contestées à l'appui de cette inconstitutionnalité lorsque la préservation de l'ordre public le justifie, le Conseil constitutionnel invalide l'objet de la norme constitutionnelle (art. 2 de la Déclaration de 1789) à s'appliquer en l'espèce et fait naître la prescription « si une inconstitutionnalité entraîne des effets manifestement excessifs au détriment de la préservation de l'ordre public (F), alors la violation de la Constitution ne peut pas obtenir d'application (C) ». Dans ce cas, une PE naît d'une invalidation de la PE à exécuter, et elle prend systématiquement la forme « si (F), alors la règle invoquée ne peut pas être validée (C) ». En présence d'une telle règle d'invalidation, une discordance majeure peut se produire entre le F de la prescription à exécuter (art. 2 Déclaration de 1789) et le F de la prescription exécutée (règle d'invalidation), mais la raison d'être de cette discordance est précisément l'invalidation de la prescription à exécuter. Autrement dit, une telle discordance ne peut se produire que si la prescription à exécuter est invalidée, arrêtée dans son parcours prescriptif avant de pouvoir obtenir application, voire ici relayée par une nouvelle PE créée par invalidation. Par conséquent, une PE ne peut effectivement obtenir réalisation que si son cadre factuel est relativement stable tout au long de son parcours.

404« En complément » parce que nous n'étudions pas l'interprétation dans le même contexte que M. Troper : M. Troper tente d'expliquer la cohérence interprétative entre les décisions rendues par le juge ; nous tentons ici d'expliquer la cohérence interprétative entre des prescriptions étatiques qui découlent les unes des autres pour permettre l'accomplissement d'une prescription de départ.



Une telle modélisation appelle plusieurs remarques. Premièrement, elle transcrit les caractéristiques du processus de réalisation d'une PE. On insiste sur trois d'entre elles. Pour commencer, le **parcours prescriptif** concret de PE-1 est **interrompu** par la création abstraite de nouvelles prescriptions. Ainsi qu'on l'a déjà relevé pour la modélisation simple, toute création prescriptive doit traverser une phase abstraite avant d'entrer dans une phase concrète. Dans la modélisation proposée, l'exécutant (Cour EDH, gouvernement, préfet, policier) doit abstraitement poser une règle exécutable et applicable (par arrêt de justice, circulaire, arrêté, agissement habilité) avant que cette règle puisse être concrètement exécutée et appliquée (par le gouvernement, le préfet, le policier). Le trajet prescriptif *concret* de PE-1 est alors discontinu, entrecoupé en cours par une série d'épisodes *abstraits* de créations prescriptives. En interrompant ainsi le parcours de réalisation de PE-1, chaque nouvelle prescription se substitue abstraitement à la précédente et modifie de la sorte la signification abstraite précédemment posée. Ce phénomène interprétatif par lequel une nouvelle signification est prêtée à la prescription interprétée rend ensuite le **parcours prescriptif** concret de PE-1 **sinueux**. La modélisation est à ce propos marquée par des rebonds, chacun se produisant lorsqu'une nouvelle prescription est créée par interprétation de la précédente. Les prescriptions ainsi créées par interprétation mènent finalement le **processus prescriptif** concret de PE-1 à être **dévié**. Par interprétations successives qui font se substituer une nouvelle prescription à la précédente, la trajectoire prescriptive de PE-1 est inclinée de manière que la réalisation concrète de PE-1 ne peut être alignée sur le même niveau que sa création abstraite. Pour résumer, le parcours prescriptif discontinu, sinueux et dévié d'une PE se traduit par une trajectoire interrompue, rebondie et inclinée, symbolisant ainsi **l'impossibilité pour une PE de préserver son intégrité à travers un processus interprétatif**.

Deuxièmement, cette modélisation complexe offre d'identifier les divers prescripteurs étatiques. En définissant le **prescripteur** comme le **producteur d'une prescription**, on note trois manières de produire des prescriptions étatiques d'après cette modélisation : la création de la règle abstraite ; son exécution ; et son application. À la lecture de la modélisation complexe, seules ces trois activités sont sources de prescriptions. Les autres acteurs prenant part au processus de réalisation d'une PE (comme l'intervenant factuel ou encore l'auteur de la sollicitation) n'étant pas producteurs de prescriptions étatiques, on en déduit que **le créateur de la règle de droit, son exécutant et son applicateur sont les prescripteurs exclusifs participant à la réalisation d'une prescription étatique**. Pour la suite de la thèse, le « prescripteur étatique » désignera donc nécessairement ce créateur, cet exécutant ou cet applicateur de la PE.

Paragraphe 2 – Comparaison avec la modélisation complexe du processus prescriptif numérique

On rappelle qu'on a tenu pour « prescriptions numériques » les règles issues du langage-machine (règles machine) au moment où elles deviennent exécutables et applicables. Comme pour la prescription étatique, la prescription numérique (PN) peut, d'ici à son accomplissement, interférer avec d'autres PN durant son parcours prescriptif. Ces interférences sont évidemment démultipliées lorsque la PN étudiée emprunte un réseau numérique qui la fait traverser plusieurs exécutants jusqu'à sa réalisation concrète. Compte tenu de notre objet d'étude, nous nous focaliserons sur les interférences permises par le réseau internet. L'échelle de ce réseau, qui dépasse de loin celle locale d'une seule machine numérique, facilite de nombreuses interactions de PN, et pas seulement des PN incarnées par des règles machine.

Les éléments définitoires d'une prescription numérique sont en effet satisfaits dès qu'une règle conditionnant une conséquence numérique C (réaction d'une machine numérique) par un fait numérique F (suite binaire) est numériquement exécutable et applicable (associée à un mécanisme numérique d'exécution et d'application tel le processeur). Toute règle logicielle (ou instruction logicielle), quel qu'ait été son programmeur/développeur, réunit ces caractéristiques d'une PN⁴⁰⁵.

On a vu qu'une instruction logicielle est formée par des symboles humainement compréhensibles qui combinent plusieurs instructions préalables ou machine pour créer une nouvelle fonction (par exemple, la fonction « calculer l'adresse effective d'une instruction », symbolisée par la mnémotique LEA et combinant plusieurs instructions machine de calcul). L'instruction logicielle n'est pas comprise par la machine : seules les règles machine qu'elle combine sont directement exécutables et applicables par le processeur. La règle logicielle (instruction logicielle) se situe donc à un niveau d'abstraction supérieur à celui de la règle machine (instruction préalable ou machine), en ce sens qu'elle s'abstrait de la compréhension machinale. Elle n'est pas rédigée en code binaire, mais en langage informatique, de sorte que deux instructions logicielles sont compatibles (ou interopérables) à travers les symboles qu'elles emploient, à travers le langage informatique qu'elles mobilisent.

Pour illustrer les caractéristiques prescriptives des instructions logicielles à travers internet, on se référera au cas JVC précité, forum en ligne dont le logiciel rend possible la publication de caractères alphabétiques étrangers ou issus de langues mortes (ă, ș, ă...). On examine ici le cas concret d'un internaute qui, depuis son navigateur web, veut publier des caractères alphabétiques étrangers ou issus de langues mortes sur le forum JVC. Comment peut-il accéder à cette fonction logicielle hébergée sur le serveur de JVC ? Il doit produire et faire exécuter une PN concrète, *i.e.* une requête d'accès. Cela demande de convertir un certain nombre de PN abstraites en requêtes d'accès⁴⁰⁶. On retracera ici le parcours de la requête d'accès produite par l'utilisateur et destinée au serveur de JVC pour publier le message « șăle măr2e ».

⁴⁰⁵ Communément, une instruction logicielle est un extrait du code source qui génère une fonctionnalité. Basiquement, l'instruction `if (x > 0) { result = 'positive'; }` représente l'unité formelle d'une instruction logicielle qui entraîne une conséquence « positive » chaque fois que la condition `(x > 0)` se vérifie. Le développeur peut compléter cette instruction par l'instruction `else { result = 'NOT positive'; }` qui ouvre la possibilité d'une autre conséquence que celle positive prévue lorsque la condition `(x > 0)` ne se vérifie pas.

⁴⁰⁶ Rappelons que la phase abstraite d'une PN est constituée par deux étapes : l'énoncé de la règle contenu dans le code-source du logiciel a d'abord été posé par l'auteur de ce logiciel ; cette règle a ensuite acquis la qualité de prescription en étant associée à un mécanisme d'exécution et d'application

Pour produire cette requête, l'utilisateur doit d'abord se servir d'un système d'exploitation. Grâce au système d'exploitation, l'utilisateur peut utiliser les logiciels installés sur son terminal – et peut donc utiliser un navigateur web sur son terminal pour communiquer sa requête au serveur de JVC. À cette fin, le système d'exploitation comporte la règle logicielle : « *si l'utilisateur allume son ordinateur et clique sur l'icône de son navigateur web (F), alors le processeur doit exécuter les données produites pour faire s'afficher sur l'écran la fenêtre proposée par ce navigateur (C)* »⁴⁰⁷. On s'attardera sur cette première règle pour vérifier que la règle logicielle est prescriptive au même titre que la règle machine.

En l'espèce, l'utilisateur produit des données binaires (intervention factuelle) afin d'ouvrir son navigateur web ; en demandant la possibilité d'utiliser cette fonctionnalité du système d'exploitation, l'utilisateur émet une requête logicielle d'accès (sollicitation) au système d'exploitation pour que soit exécutée la règle nous servant d'exemple (l'exécution est donc suscitée par le croisement d'une sollicitation avec une intervention factuelle) ; le terminal qui stocke cette règle logicielle du système d'exploitation vérifiera la validité en l'espèce de la sollicitation émise (la requête parvient-elle dans un format recevable ?), de la règle ainsi requise (est-elle mathématiquement cohérente avec les autres règles stockées et son résultat est-il identique à celui attendu pour la même règle stockée par le terminal ?) et du fait F qui en conditionne l'application (les données binaires produites par l'internaute, i.e. l'intervention factuelle, correspondent-elles à un clic sur l'icône du navigateur web, i.e. au F de la règle invoquée ?). On a constaté que, durant cette triple validation, la machine numérique est neutre : les incertitudes pesant sur l'état prescriptif de la règle sont levées sans que la validation soit orientée par les décisions de l'exécutant. Pour l'illustration qui nous occupe, le terminal hébergeant le système d'exploitation vérifie la recevabilité de la requête en s'assurant que son format est *identique* à celui d'un datagramme IP, valide la règle dont l'exécution est requise en constatant qu'elle est formellement *identique* à celle qu'il héberge et mathématiquement cohérente avec les autres règles stockées par la machine, et déduit son applicabilité au cas concret de l'*identité* entre les bits produits par l'intervention factuelle et ceux qui composent le F de ladite règle.

Comme on l'avait observé pour la règle machine (dont la validité est impliquée par la validité de la requête d'accès en langage machine), la validité de la règle logicielle est elle aussi liée par celle de sa sollicitation (requête logicielle d'accès) : valider la requête logicielle d'accès revient à valider la règle logicielle. Ces considérations nous amènent à confirmer qu'aucune décision de l'exécutant numérique ne s'immisce entre ces deux validations, et que la troisième validation procède d'une correspondance chiffrée et identique entre l'intervention factuelle et le F de la règle sollicitée. Le terminal agit en exécutant neutre de la règle logicielle sollicitée, incapable de lui prêter une nouvelle signification. Se produit alors un « **phénomène d'interopérabilité machinale** » qui, supplantant le phénomène interprétatif, consiste à **achever une opération numérique par effet de médiations inter-machinales**. Tandis que les médiations sociales interhumaines conduisent généralement à valider une PE par *approximation des significations* (phénomène interprétatif), les médiations numériques inter-machinales conduisent nécessairement à valider une PN par *identité des données* et *cohérence mathématique* (phénomène d'interopérabilité). Seules les requêtes d'accès identiques (aux données programmées) et mathématiquement cohérentes (avec les autres règles programmées) étant valides, tout changement

⁴⁰⁷ Les exemples de prescriptions numériques seront évidemment extrêmement simplifiés tout au long de notre démonstration, car de nombreuses instructions logicielles sont en réalité impliquées pour aboutir au résultat ici mentionné

de signification apportée par l'exécutant numérique à ces données altérerait de fait leur identité et leur cohérence et empêcherait leur validation par interopérabilité. En résumé, par phénomène d'interopérabilité, **l'exécutant numérique validant une PN ne peut signifier aucune nouvelle prescription.**

On en conclut que la validation par interopérabilité est le moyen qui préserve la neutralité de l'exécution. Ainsi préservée, la neutralité de l'exécution déploie un effet notable, inconnu de l'exécution étatique : elle crée une aliénation de l'exécutant numérique à la requête le sollicitant. Cette originalité se vérifie à chacune des trois étapes classiques de l'exécution dans le cas concret, qui n'autorisent pas le moindre espace à l'appréciation de l'exécutant entre la requête émise et l'application de la règle.

En premier lieu, la validation par interopérabilité d'une sollicitation ne permet aucun écart entre cette sollicitation et ses conditions de validité, les deux devant être *formellement identiques*. Le lien d'identité entre la sollicitation et ses conditions de validité est alors déterminé dès l'instant où la sollicitation joint la règle pour en demander l'exécution, soit avant même l'exécution effective. L'identité entre la sollicitation et ses conditions de validité n'est donc pas déterminée par l'exécutant, mais prédéterminée au stade de la requête émise : si la requête correspond au format exigé, elle est valide ; si elle n'y correspond pas, elle est invalide. D'une part, l'identité de la sollicitation à ses conditions de validité étant prédéterminée, aucun espace interprétatif n'est laissé à l'exécutant pour apprécier la satisfaction de ces conditions par la requête. D'autre part, cette identité prédéterminée étant établie par la requête, la *validation* de cette requête par l'exécutant est aliénée à sa *validité* préalable. En somme, par combinaison d'une neutralité de l'exécution et d'une identité prédéterminée de la sollicitation à ses conditions de validité, **l'issue de l'exécution d'une requête** (validation (action)/invalidation (inaction)) **est exclusivement tributaire de cette requête** (préalablement valide/invalide, le processeur ne faisant que constater cette validité ou invalidité préalable).

En second lieu, la validation par interopérabilité d'une règle ne permet aucun écart entre la règle dont l'exécution est sollicitée (telle qu'elle parvient à l'exécutant) et la règle dont l'exécutant connaît la validité (telle que stockée par la mémoire), les deux devant être *formellement identiques*. De la même manière, la validation par interopérabilité d'une règle ne permet aucune incohérence mathématique entre la règle dont l'exécution est sollicitée et les autres règles stockées par la mémoire. En effet, la cohérence mathématique entre la règle à exécuter et les autres règles stockées, ainsi que l'identité entre la règle reçue et la règle stockée, permettent d'en déduire aussi bien la valeur prescriptive de la règle dans le cas concret que son objet à s'appliquer dans le cas concret. D'abord, si la règle à exécuter et la règle hébergée sont associés à des mécanismes d'exécution et d'application identiques, c'est donc que ces deux règles appartiennent au même système exécutif connu et gardé par l'exécutant sollicité, au titre de laquelle appartenante la règle identiquement concernée est pourvue d'une valeur prescriptive dans le cas concret. En l'espèce, la valeur prescriptive de la règle logicielle dont l'exécution est sollicitée (affichage de la fenêtre du navigateur) résulte ainsi de l'identité entre la machine dont le processeur exécute la règle et la machine qui stocke cette règle. Ensuite, si la règle reçue et la règle hébergée sont rapportables à un objet identique (*i.e.* à une même unité $F \rightarrow C$), c'est donc que la règle identiquement concernée a pour objet de s'appliquer au cas concret. En l'espèce, l'objet de la règle logicielle à s'appliquer dans le cas concret résulte ainsi de l'identité entre l'unité formelle sous laquelle la règle est communiquée au serveur exécutant (l'instruction logicielle dont l'utilisateur demande l'exécution) et l'unité formelle sous laquelle la règle est hébergée par le serveur

exécutant (l'instruction logicielle rédigée par le programmeur). D'une part, la règle à exécuter devant être identique à celle hébergée pour être valide, aucun espace interprétatif n'est laissé à l'exécutant pour apprécier la valeur prescriptive et l'objet de la règle dans le cas concret. D'autre part, la règle à valider dans le cas concret n'étant pas la règle hébergée (dont la validité déjà acquise du seul fait de son hébergement ne peut être altérée par l'exécutant neutre) mais la règle reçue par le processeur, c'est seulement sur cette règle reçue que pèse l'incertitude de la validité de la règle dans le cas concret. En d'autres termes, la validation de la règle dans le cas concret dépend des mécanismes d'exécution-application et de l'objet (navigateur web et instruction logicielle d'ouverture du navigateur) *tels que déterminés par la requête* porteuse de la règle à valider. À cause de la neutralité de l'exécutant qui lui interdit toute appréciation dans la validité de la règle hébergée et dans l'identité entre les règles reçues et hébergées, **la validité de la règle dans le cas concret est tributaire non des déterminations** faites par l'exécutant mais de celles **faites par la requête** : une règle invalide dans le cas concret est le fruit d'une requête elle-même invalide tout comme une règle valide dans le cas concret est le fruit d'une requête elle-même valide.

En troisième lieu, la validation par interopérabilité de l'applicabilité de la règle ne permet aucun écart entre l'intervention factuelle et le F de la règle, les deux devant être *formellement identiques*. On sait en effet que cette applicabilité se déduit classiquement du remplissement de F dans le cas concret, *i.e.* de sa correspondance avec l'intervention factuelle survenue. Cependant, une remarque supplémentaire doit être faite à ce sujet : le F d'une PN est identique aux conditions de validité de la sollicitation, de façon que la validation de la requête implique elle aussi le remplissement de F. Pour reprendre notre exemple de l'« instruction R » donné dans la modélisation simple, on a vu que la requête d'accès à cette instruction s'écrit 10100000 00000001 01010010. On a vu aussi que la requête d'instruction correspond à la règle suivante : « *si l'utilisateur produit les bits 10100000 00000001 01010010 (F), alors le processeur doit incrémenter et additionner 00000001 et 01010010 dans le registre A (C)* ». Par conséquent, les conditions de validité de la sollicitation sont incluses dans le F de la règle : l'enclenchement de C est exclusivement conditionné par la validité de la sollicitation. La sollicitation qui est identique au F de la règle est donc par-là même identique à ses conditions de validité. La validation de la sollicitation et celle de l'applicabilité de la règle dans le cas concret ont alors pour source commune la validation de la requête. Pour le dire autrement, si la requête est validée, sont du même coup validées la sollicitation et la possibilité d'appliquer la règle dans le cas concret. Il en va de même pour une requête logicielle : pour rester sur la règle logicielle prévue par le système d'exploitation, l'affichage de la fenêtre du navigateur web (C) est conditionné par la validité de la requête d'accès au navigateur web (F). D'une part, l'applicabilité de la règle se déduisant d'une identité de l'intervention factuelle et du F de cette règle, aucun espace interprétatif n'est laissé à l'exécutant pour apprécier le remplissement de F dans le cas concret. D'autre part, l'identité du F de la règle et de l'intervention factuelle tenant à une requête valide, la requête valide constitue la condition du remplissement de F dans le cas concret. Ainsi combiné à la neutralité de l'exécution, le remplissement de F exclusivement conditionné par la validité de la requête rend **l'applicabilité de la règle dans le cas concret exclusivement tributaire d'une requête valide**.

Pour chacun des temps de l'exécution, on observe que **la neutralité de l'exécutant numérique a pour effet d'aliéner son travail de validation à la validité de la requête**. La **validité** (dans laquelle l'exécutant n'intervient pas) **et la validation** par interopérabilité (qui prive l'exécutant d'espace interprétatif) **de la requête emportent respectivement validité et validation**

de la sollicitation, de la règle dans le cas concret et de la possibilité de l'appliquer à ce cas. On confirme donc que la prescription numérique possède les mêmes propriétés de validation, qu'elle soit émise dans le cadre d'une requête d'accès en langage machine ou d'une requête logicielle d'accès. Cette confirmation, qui singularise la PN par rapport à la PE, a d'importantes répercussions sur une modélisation complexe car elle permet de comprendre comment **l'interopérabilité, en préservant la neutralité de l'exécutant, préserve par-là même l'intégrité de la PN** qui traverse plusieurs exécutants sur internet.

En effet, à l'échelle du réseau internet, d'autres exécutants que le terminal de l'utilisateur s'immiscent dans le parcours de la requête d'accès à la règle logicielle hébergée par le serveur de JVC. Une fois que l'utilisateur a fait ouvrir la fenêtre de son navigateur web, il peut l'utiliser pour accéder au service JVC. Le navigateur sert ici de logiciel client pour que l'utilisateur puisse communiquer avec le serveur JVC. Le client est programmé avec des instructions qui permettent de structurer des requêtes IP d'accès. Le navigateur est donc programmé avec la règle : « *si l'utilisateur produit les données constitutives pour la formation d'une requête IP d'accès (F), alors le processeur doit vérifier que la structure de la requête est exacte (C)* ». Il s'agit ici d'une PN abstraite, c'est-à-dire d'une PN hypothétiquement applicable indépendamment de tout cas concret, et qui ne trouvera exécution qu'en présence d'un cas concret (si survient une intervention factuelle qui sollicite cette exécution). On appellera cette prescription « PN-0 ». Sur le fondement de PN-0, l'utilisateur peut donc produire la requête IP suivante :

Requête (logicielle) d'accès IP			
Protocole de communication utilisé	Adresse IP de l'émetteur	Adresse IP du destinataire	DATA (données destinées à être exécutées par le destinataire)
IP	Terminal de l'utilisateur	Serveur de JVC	Clic [sur la fonction publication] et message « şăle mër2e »

On peut aussi décrire cette requête selon la règle suivante : « *si l'utilisateur du terminal portant telle adresse IP demande à la machine portant l'adresse IP destinataire de publier le message "şăle mër2e" (F), alors la machine destinataire des données à exécuter doit exécuter ce message en lui appliquant les effets qu'elle prête au clic [publication du message en l'espèce] (C)* ». On appellera cette règle « PN-1 » : c'est la première prescription qui porte la requête d'accès de l'utilisateur destiné au serveur de JVC.

Le terminal de l'utilisateur n'exécutera pas PN-1, car il n'est pas le destinataire d'une telle requête et ne saurait donc appliquer la conséquence C de PN-1. En revanche, il vérifiera que la forme du datagramme IP est exacte (si un protocole de communication valide est indiqué, si la bonne adresse IP émettrice est renseignée, si l'adresse IP destinataire est correctement formulée, si le champ DATA est rempli par des données valides stockées par le terminal...). En vérifiant l'exactitude de la structure de la requête, le processeur exécute donc PN-0. Cela signifie que **PN-0 (PN abstraite) est exécutée à travers la production de PN-1 (PN concrète).**

Or, l'exécution de PN-0 appelle une autre PN abstraite. En effet, le navigateur stocke également sur le terminal la règle suivante : « *si la requête IP d'accès est destinée à un site web utilisant le protocole HTTP (F), alors doit être formulée une requête HTTP dont le processeur*

doit vérifier l'exactitude de la structure (C) ». On nommera cette règle « PN-2 »⁴⁰⁸. Sous réserve que la requête IP soit exactement formulée, l'exécution de PN-0 appelle PN-2 pour que soit formulée une requête HTTP.

Seulement, PN-2 est une règle abstraite, et ne trouve donc exécution qu'à travers une requête d'accès concrète. Le navigateur ainsi appelé à exécuter PN-2 produit donc concrètement une requête HTTP d'accès, qui cible spécialement le site jeuxvideo.com comme destinataire en l'espèce. La requête HTTP possède une structure différente de la requête IP, et communique au serveur de JVC des informations dans le langage informatique avec lequel il est programmé (basiquement HTML et ses dérivés). De cette façon, par le biais de la requête HTTP, le navigateur peut communiquer au serveur de JVC des informations qui seront comprises par le logiciel JVC afin d'exécuter la demande de publication du message. La requête HTTP est structurée différemment de la requête IP, en indiquant notamment le type de requête HTTP (type GET pour récupérer une ressource en ligne tel qu'un commentaire consulté ou le téléchargement d'un fichier, type POST pour un simple envoi de données au destinataires, type DELETE pour demander la suppression d'une ressource au serveur, type PATCH pour modifier une ressource etc.), l'url destinataire exacte ou encore la version HTTP utilisée (HTTP, HTTPS, SSL...). En produisant une requête HTTP dans le cas concret, le navigateur produit la règle suivante en l'espèce : *« si une requête HTTP ordonne un simple envoi de données vers l'url jeuxvideo.com/forums/48-31-50390430 programmée avec le protocole https (F), alors cette page web doit y répondre en confirmant la bonne réception des données envoyées (C) »*. On nommera cette PN concrète « PN-3 ».

De la même manière que la PN-1 concrète (requête IP d'accès destinée à l'adresse IP du serveur de JVC) était fondée sur le PN-0 abstraite (structuration d'une requête IP d'accès), la PN-3 concrète (requête HTTP destinée à la page web sur laquelle l'utilisateur veut publier son message) est fondée sur la PN-2 abstraite (structuration d'une requête HTTP). Et, de la même manière que la production de PN-1 a provoqué l'exécution de PN-0, la production de PN-3 provoque l'exécution de PN-2. En effet, le terminal ne peut exécuter PN-3 car il n'en est pas le destinataire et ne peut donc appliquer la conséquence C prévue par PN-3. En revanche, il vérifiera si la structure de la requête HTTP est exacte et, ce faisant, il exécute et applique PN-2.

Une fois le format de la requête HTTP validé par le terminal de l'utilisateur, les requêtes concrètes (PN-1 et PN-3) destinées au serveur de JVC peuvent lui être transmises. Le serveur de JVC commence par exécuter la requête HTTP concrète (PN-3) qui lui est destinée. Il exécute

⁴⁰⁸ On simplifie ici l'exemple pour ne pas avoir à modéliser trop d'étapes (la modélisation serait peu lisible). En pratique, avant de produire une requête IP, l'utilisateur doit adresser une requête DHCP au serveur DHCP, qui transmettra à son tour une requête au terminal de l'utilisateur pour lui attribuer une adresse IP publique (celle que la requête IP mentionnera dans le champ « adresse IP émettrice »). De même, entre l'exécution de PN-0 et l'appel de PN-2, s'intercale notamment des requêtes DNS : le navigateur comporte une règle pour structurer et vérifier l'exactitude d'une requête DNS ; cette requête DNS est reçue par les serveurs DNS qui l'exécutent ; les serveurs DNS sont eux-mêmes programmés avec des règles abstraites pour convertir l'adresse IP destinataire en nom de domaine correspondant à cette adresse IP, au nom d'hôte du destinataire et au port qu'il emprunte (port 80 pour le Web) ; l'exécution par les serveurs DNS de la requête DNS envoyé par le navigateur appelle l'exécution de cette règle abstraite de conversion, conduisant le serveur DNS à émettre à son tour une requête DNS destiné au navigateur pour l'informer du nom de domaine correspondant à l'adresse sollicitée. De cette façon, le navigateur peut connaître le nom de domaine du site web destinataire. C'est en connaissance de ce nom de domaine que le navigateur peut appeler PN-2, afin de destiner une requête HTTP au domaine jeuxvideo.com.

ensuite PN-1 qui lui est aussi destinée, c'est-à-dire la requête IP qui contient le message dont l'utilisateur demande la publication.

Le même scénario se reproduit : tout comme l'exécution de PN-0 a appelé la PN-2 abstraite, l'exécution de PN-1 appelle une nouvelle PN abstraite. En effet, comme tout site web qui permet la publication de commentaires, le logiciel JVC hébergé sur le serveur destinataire est programmé avec une règle qui permet de structurer une requête d'accès destinée à sa base de données recensant les commentaires publiés sur JVC. En l'espèce, cette règle admet le transfert, vers cette base de données, de messages comportant des caractères issus de langues étrangères ou de langues mortes. On peut la formuler ainsi : *« si sont exécutées des requêtes IP et HTTP valides prescrivant la publication d'un message (F), alors doit être formulée et vérifiée une requête d'accès destinée à la base de données réservée aux commentaires publiés sur JVC, pour transmettre ce message vers cette base de données (C) »*. On nommera cette prescription abstraite « PN-4 », appelée par l'exécution de PN-1 et PN-3.

Enfin, comme pour les autres PN abstraites, PN-4 est exécutée à travers la production d'une PN concrète fondée sur PN-4. En l'espèce, l'appel de PN-4 par l'exécution de PN-1 et PN-3 engendre la production d'une nouvelle PN concrète : la requête d'accès effectivement destinée à la base de donnée de JVC. On nommera cette requête « PN-5 », qu'on peut présenter ainsi : *« si des requêtes IP et HTTP ordonnent la publication du message "şăle mër2e" sur la page web référencée à l'url jeuxvideo.com/forums/48-31-50390430 (F), alors ce message doit être stocké dans la base de données vers laquelle pointe vers cet url (C) »*. Le serveur hébergeant le site web de JVC n'est pas lui-même destinataire de cette requête, et se cantonnera donc à vérifier que ladite requête d'accès portée par PN-5 est correctement formalisée. Il exécutera donc PN-4 à travers la production de PN-5. Puis il transmettra PN-5 au serveur qui héberge la base de données de JVC, lequel serveur pourra alors exécuter et appliquer PN-5. À l'issue de cette dernière application, le message de l'utilisateur sera donc publié à l'url ciblée, et sera donc publiquement accessible à toute personne accédant à cet url⁴⁰⁹.

La neutralité de l'exécution par un processeur et sa liaison par l'instruction machine ayant déjà été constatés pour la modélisation simple, il n'est pas utile de les rappeler ici ; de manière que **la validation de PN-5 par son exécutant est aliénée à la requête formulée par l'exécutant de PN-4, la validation de PN-4 par son exécutant est aliénée à la requête formulée par l'exécutant de PN-3, la validation de PN-3 par son exécutant est aliénée à la requête formulée par l'exécutant de PN-2, la validation de PN-2 par son exécutant est aliénée à la requête formulée par l'exécutant de PN-1, et la validation de PN-1 par son exécutant est aliénée à la requête formulée par l'exécutant de PN-0.**

En plus de la neutralité exécutive, l'exécution et l'application sont confusément effectuées par le même processeur, comme décrit par la modélisation simple ; **aucun espace interprétatif**

⁴⁰⁹ Le chemin de la requête de l'utilisateur s'arrête à cet endroit, mais le serveur hébergeant la base de données de JVC émettra à son tour une requête IP d'accès (donc produira une PN concrète) destinée au terminal de l'utilisateur, pour permettre à ce terminal de voir s'afficher sur l'écran de son terminal le commentaire ainsi publié, ou une page web confirmant la bonne publication du message. La requête IP émise par la base de données (ou par le serveur JVC lui-même après que la base de données l'ait sollicité à cette fin) fera le chemin inverse, en passant par le navigateur de l'utilisateur puis *in fine* par son système d'exploitation qui fera s'afficher la page web renvoyée en réponse à la requête IP de l'utilisateur.

n'est donc laissé entre l'exécution et l'application de PN-0, de PN-1, de PN-2, de PN-3, de PN-4, puis de PN-5.

En somme, **par phénomène d'interopérabilité, l'accomplissement de PN-5 garantit l'intégrité de PN-1**. Chaque exécutant est aliéné à la sollicitation de l'exécutant antérieur, et chaque sollicitation est valide par identités formelles consécutives avec la demande d'exécution originelle de PN-1. Du fait d'une validation par interopérabilité, **la sollicitation numérique originellement valide entraîne alors la réalisation physique exacte du C de PN-1**. De PN-1 à PN-5, la chaîne prescriptive suit un cadre conséquentiel radicalement stable grâce auquel, de validation en validation, **le C de PN-5 concorde parfaitement avec le C de PN-1**. Ainsi, **la stabilité du cadre conséquentiel assure à PN-1 une effectivité inhérente au processus prescriptif numérique** (car rapportable à ce processus dont le déroulement par interopérabilité soumet une continuité d'exécutants à une validation neutre de la requête par identités des opérations).

L'interopérabilité n'est pas la seule cause d'effectivité ou d'ineffectivité d'une PN. On en identifie une autre : pour que la PN puisse produire ses effets, le processeur doit être capable de les traiter (ne pas être victime d'un problème de ventilation de la machine, d'une saturation des registres par une quantité excessive de données etc.). Dès lors, pour autant que le processeur est *capable* de traiter les données, l'effectivité d'une PN dépend seulement de l'interopérabilité des données à exécuter. Ainsi, **l'utilisateur peut toujours accéder à la fonctionnalité proposée par JVC** (PN-4, publication de messages sur le forum, y compris ceux qui contiennent des caractères spéciaux) **quelles que soient les règles qu'il mobilise⁴¹⁰, du moment que toutes ces règles sont valides par interopérabilité et que les processeurs des machines empruntées sont capables d'exécuter les données**.

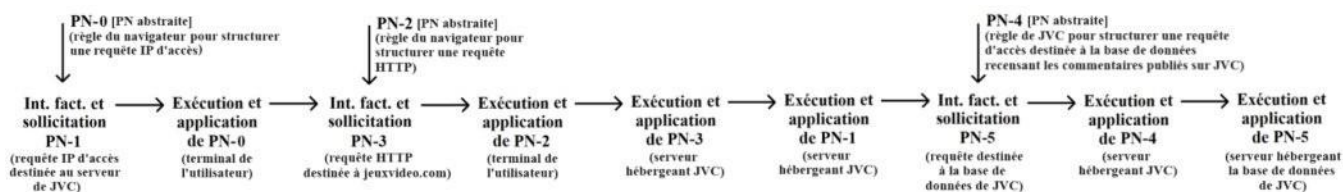
En évaluant cette effectivité selon les effets emportés par PN-1 auprès de l'applicateur, on observe d'abord une effectivité totale : l'applicateur final et les exécutants antérieurs sont liés par la règle dans son intégralité, de son F jusqu'à son C, au sein d'un cadre conséquentiel stable. Cette effectivité est ensuite absolue parce qu'une seule et unique application peut être faite de la règle – celle qui permet la réalisation physique du C de PN-1. PN-1 ne peut donc être appliquée de manière nuancée par rapport à la conséquence qu'elle prévoit : soit elle est appliquée d'une manière parfaitement identique au C énoncé, soit elle ne l'est pas du tout. Enfin, l'effectivité de PN-1 à l'échelle de son parcours prescriptif est intègre : de sa sollicitation à son application, elle n'est biaisée par aucune des interventions des autres PN ni par celles de leurs exécutants. Tout comme l'application elle-même, chaque exécution est connectée à la précédente *via* une cohérence exacte d'opérations numériques validées à l'identique.

En comparaison, d'un côté, **l'effectivité processuelle de la PE est (i) partielle** par son étendue limitée au fait de conditionnement F de PE-1, **(ii) relative** par la diversité et les nuances de ses applications et **(iii) déviée** par l'approximation de sa cohérence. De l'autre, **l'effectivité processuelle de la PN est (i) totale** par son étendue incluant la conséquence C de PE-1, **(ii) absolue** par l'unicité de son application et **(iii) intègre** par l'exactitude de sa cohérence. De

⁴¹⁰ L'utilisateur peut ainsi mobiliser les PN du système d'exploitation Windows, macOS (Apple) ou Android, tout comme il peut mobiliser les PN du navigateur Safari, Chrome, Kiwi, Arc, Firefox... De la même manière, il peut utiliser l'application mobile de JVC qui jouera le rôle de client, auquel cas l'utilisateur n'aura pas besoin d'utiliser un navigateur pour accéder au site web de JVC, il peut emprunter les règles de routage de différents opérateurs, ou les règles de conversion des adresses IP du résolveur DNS de son choix etc. Pour faire exécuter PN-4, peu importe les règles mobilisées du moment qu'elles sont interopérables.

cette comparaison entre la phase concrète de réalisation d'une PN et celle d'une PE, on en déduit que **l'effectivité de la PN est, pour chacune de ses caractéristiques, structurellement (processuellement) supérieure à celle de la PE** en ce sens que les effets attachés à une PN lui assurent une exacte réalisation plus complète, plus sûre et plus fidèle.

On aboutit à la modélisation complexe suivante :



Phase concrète de PN-1

Une telle modélisation appelle plusieurs remarques. Premièrement, les caractéristiques qu'elle révèle du parcours prescriptif concret de PN-1 sont totalement inverses à celles relatées par la modélisation du parcours prescriptif concret d'une PE. Pour commencer, le **parcours prescriptif** concret de PN-1 est **ininterrompu**. Aucun épisode abstrait n'en brise la continuité : les prescriptions tierces n'intègrent pas le trajet de PN-1, elles lui restent extérieures au moment d'interférer avec. La création des prescriptions abstraites se situe en-dehors du parcours de PN-1. Aucune de ces créations prescriptives tierces ne résulte d'une nouvelle signification prêtée à l'une des prescriptions impliquées et la signification abstraite de PN-1 en ressort alors parfaitement intacte jusqu'à sa réalisation. Les significations abstraites des prescriptions tierces s'ajoutent à celle de PN-1 durant son itinéraire sans s'y substituer. Ainsi débarrassé de tout intermède abstrait de création prescriptive qui l'entrecouperait, le **parcours prescriptif** concret de PN-1 s'illustre ensuite par un tracé **rectiligne**. Au lieu de la trajectoire rebondie obtenue dans la modélisation complexe d'une PE, on découvre au contraire une trajectoire dont l'allure plate n'est aucunement perturbée par les créations prescriptives interférant avec PN-1. Ces interférences n'ayant dès lors pas pour effet de dévier le cheminement de PN-1, son **parcours prescriptif** concret est parfaitement **linéaire**. La trajectoire de PN-1 se dessine droite de manière que sa création abstraite est parfaitement alignée sur sa réalisation concrète. En comparaison, tandis que le phénomène interprétatif provoque une trajectoire discontinue, rebondie et inclinée de la PE, le phénomène d'interopérabilité donne lieu à une trajectoire continue, plate et droite symbolisant **l'intégrité inaltérée de la PN d'ici sa réalisation**.

Deuxièmement, comme la modélisation complexe de la PE, celle de la PN permet d'identifier les divers prescripteurs numériques. En maintenant notre définition du prescripteur comme le producteur d'une prescription, on extrait de cette modélisation complexe de la PN deux façons de produire des prescriptions numériques en ligne : la création de règles abstraites ; et la production de données concrètes. La création de règles abstraites consiste à poser des règles dont le format informatique, octroyé soit par langage logiciel soit par langage machine, en fait des règles exécutables et applicables par une machine numérique. Emprunter cette voie pour prescrire en ligne n'autorise toutefois à produire que des **prescriptions abstraites qui ne dépassent pas la deuxième étape de leur parcours prescriptif**. Complémentairement, la

production de données concrètes consiste à générer en ligne des données binaires, soit par automatisation logicielle soit par une action manuelle, dont la traduction finale en instruction machine ordonne l'application d'une règle et en aliène l'exécution. Emprunter cette voie pour prescrire en ligne n'autorise toutefois à produire que des **prescriptions concrètes dont l'auteur ne peut déterminer la signification abstraite qui leur est préalablement attribuée**. Dans notre exemple modélisé de JVC, pour former le message qu'il entend publier, l'internaute produit manuellement une prescription combinant des règles logicielles connues de la machine locale (règles machines relatives aux saisies de caractères) et une règle logicielle connue de l'hébergeur de JVC (fonctionnalité de publication sur le forum, incarnée par PN-1). Cette combinaison de règles abstraites est transformée en instruction machine à travers le processus étudié afin d'aboutir à l'exécution-application de ces règles. L'internaute n'a pas rédigé la règle PN-1, pas plus qu'il n'a rédigé les règles de saisie de caractères dont il ordonne l'exécution en écrivant son message. C'est pourtant bien lui et lui seul qui, en émettant un ordre concret d'application dont la machine ne peut s'écarter, prescrit à cette dernière l'exécution et l'application de règles abstraites.

Ces deux façons de prescrire en ligne (création d'une règle abstraite et production de données concrètes) sont complémentaires et même indispensables l'une à l'autre : une prescription abstraite (par ex. une fonctionnalité de saisie de caractères établie par une règle machine ou une fonctionnalité de publication de caractères alphabétiques spéciaux établie par une règle logicielle) est incapable de se concrétiser sans production de données (par ex., une saisie de caractères combinée avec une règle logicielle), et une prescription concrète est improductible sans création préalable d'une règle abstraite. Ainsi, bien qu'une production de données (automatisée ou manuelle) ne soit pas en elle-même créatrice d'une règle abstraite, le producteur de données n'en est pas moins producteur d'une prescription concrète et, en cela, prescripteur.

En examinant le cas JVC par le prisme de la modélisation complexe du processus prescriptif numérique, on peut donc identifier l'internaute comme un prescripteur numérique en qualité de producteur de prescriptions concrètes (requêtes d'accès). Plus généralement, en nous en tenant au critère de production prescriptive, on discerne quatre types de prescriptions numériques : les PN issues de la création abstraite d'une règle machine (**PN abstraites machinales**) ; celles issues de la création abstraite d'une règle logicielle (**PN abstraites logicielles**) ; celles issues d'une production manuelle de requêtes d'accès (**PN concrètes manuelles**) ; et celles enfin issues d'une production automatisée de requêtes d'accès (**PN concrètes automatisées**).

En comparaison, d'un côté, les PE trouvent deux sources de production (création de la règle de droit et interprétation de la règle par l'exécutant et l'applicateur), de quoi il en découle trois catégories de prescripteurs étatiques (le créateur de la règle, l'exécutant de la règle et l'applicateur de la règle). De l'autre côté, les PN trouvent deux sources de production (création de règles machines/logicielles et production manuelle/automatisée d'une sollicitation), de quoi il en découle trois autres catégories de prescripteurs numériques (le prescripteur machinal par sa création de règles machines, le prescripteur logiciel par sa création de règles logicielles, et le prescripteur concret par sa production manuelle ou automatisée de sollicitations). Si les PE et PN partagent la même première source de production prescriptive (la création de règles abstraites), leur deuxième source de production diverge. Par phénomène interprétatif, *la deuxième source de production d'une PE provient d'un acte d'interprétation* et confie ainsi le pouvoir de produire des PE aux interprètes (exécutant et applicateur). Or, par phénomène d'interopérabilité, *la deuxième source de production d'une PN provient d'une sollicitation* aliénante pour un exécutant-applicateur neutre alors privé du pouvoir de produire des PN, remettant ainsi ce pouvoir au producteur de données auteur de la sollicitation (prescripteur concret).

Face au **trptyque de prescripteurs étatiques créateur-exécutant-applicateur**, on reconnaît un **tryptique de prescripteurs numériques machinal-logiciel-concret**. Ces prescripteurs numériques identifiés, comment s'exerce leur pouvoir prescriptif en ligne ? On observera que les particularités avec lesquelles s'exerce ce pouvoir tiennent de lois internes à la machine numérique.

Section 2. Prescriptions numériques internes et rapports de force interhumains externes

Les caractéristiques jusque'à présent identifiées chez la PN nous fournissent les connaissances suffisantes pour interroger, en les expérimentant, nos deux hypothèses de travail faites par analogie avec la découverte de la physique quantique : existe-t-il des lois qui régissent l'activité numérique interne à la machine ? (Paragraphe 1) Et ces lois internes influencent-elles les rapports de force inter humains extérieurs à cette activité ? (Paragraphe 2)

Paraphe 1 - Les lois internes à l'activité numérique

L'accès au réseau internet s'effectuant nécessairement depuis une machine-hôte, on différencie deux types de lois internes : celles qui régissent l'activité locale de cette machine-hôte, connectée ou non au réseau numérique (A) ; et celles qui régissent l'activité en réseau de la machine connectée à internet (B).

A) Lois internes imputables à la structure numérique locale d'une machine-hôte (« lois internes locales »)

Grâce aux modélisations du processus prescriptif numérique, on sait que **la machine numérique abrite une activité** (i.e. un procédé systématique et méthodique d'actions ici machinales) **prescriptive** (ce procédé d'actions vise à réaliser une prescription : énonciation d'une règle associée à un mécanisme préexistant d'exécution, survenance d'une intervention factuelle, sollicitation, validation, application) **interne** (cette activité résulte d'une compréhension machinale qui conçoit les données binaires comme des prescriptions et agit en conséquence). Cela permet d'en conclure que **la machine numérique obéit non seulement à une activité externe** (exogène-pragmatique, saisie par la compréhension humaine) **mais également à une activité interne** (endogène, saisie par la compréhension machinale). Bien que la littérature scientifique étudiant les rapports de force en ligne réserve généralement le mot « prescription » à l'activité prescriptive externe faite de la machine numérique (par ex., les usages numériques prescrits par l'offre commerciale⁴¹¹), on relève ainsi que l'activité interne à cette machine porte également la caractéristique d'être prescriptive. Pour autant, selon leur provenance interne ou externe à la machine, ces prescriptions sont dissemblables dans leur effectivité : une prescription ne produira pas les mêmes effets si elle s'épanouit dans le monde social ou bien dans le monde numérique, ces deux mondes n'étant pas régis par les mêmes lois.

On en fera ici l'observation en retraçant, à partir des caractéristiques connues de la PN, ces lois qui régissent proprement l'activité interne de la machine numérique. Diffusée en ligne, la PN suscite en réalité deux types d'activités internes à la machine : une activité locale attribuable

⁴¹¹ On l'a particulièrement constaté *supra* en sociologie des usages, notamment à travers les écrits de Françoise PaquienSéguy qui se réfère plusieurs fois au concept de « prescription » afin de désigner le pouvoir dont dispose le concepteur de l'objet technique pour déterminer les capacités de l'utilisateur (PAQUIENSÉGUY Françoise, « L'utilisateur/consommateur producteur de richesse » in AGOSTINELLI S., AUGÉY D. et LAURIE F. (dir.), *La richesse des réseaux numériques*, préc., Presses Universitaires d'Aix-Marseille, 2012, p. 230-236 ; et PAQUIENSÉGUY Françoise, « L'utilisateur et le consommateur à l'ère numérique », in VIDAL Geneviève (dir.), *La sociologie des usages*, 2012, p. 191-192)

à la machine-hôte (qui permet la production et l'application d'une PN en ligne), et une activité en réseau attribuable aux machines interconnectées (qui permettent l'exécution en ligne de la PN entre sa production et son application). Les lois auxquelles est soumise une PN en ligne se répartissent donc en deux groupes, le premier groupe rassemblant les lois qui régissent l'activité locale, et le second celles qui régissent l'activité en réseau. Leur dissociation est d'autant plus primordiale que ces deux groupes de lois internes ne fournissent pas à la PN les mêmes apports en effectivité, *i.e.* édictent des modalités différentes pour qu'une PN posée abstraitement trouve une application concrète.

Régissant l'activité locale de la machine-hôte, le premier groupe de lois est valable pour toute PN, en ligne ou non. Les modélisations processuelles nous ont d'abord amené à éprouver une **loi de la neutralité exécutive** en vertu de laquelle **l'exécution d'une PN n'autorise pas d'écart formel**. On a vu que la validation d'une PN consiste à établir une identité entre formats (suites binaires, datagrammes, instructions logicielles...), anéantissant toute probabilité d'un écart formel dans lequel pourrait s'insérer une appréciation de l'exécutant validateur. En d'autres termes, cette loi rend improbable qu'une PN valide le soit à l'issue d'une appréciation de l'exécutant. Ainsi, la loi de neutralité exécutive implique à la fois l'intégrité de la PN vis-à-vis de l'exécutant (volet positif de la neutralité) et l'incapacité de cet exécutant à produire des PN supplémentaires (volet négatif). Inversement, une telle loi est impraticable pour la validation de prescriptions étatiques. L'absence d'identité formelle entre l'ensemble des éléments de validation d'une PE (la sollicitation et ses conditions de validité, la règle énoncée et le cas concret dans lequel son exécution est demandée, l'intervention factuelle et le fait de conditionnement de la règle) oblige son exécutant à évaluer la correspondance de ces éléments à coups d'appréciations. Cette absence d'identité formelle engendre une loi de la partialité exécutive qui implique à la fois l'impossibilité pour la PE de conserver son intégrité vis-à-vis de l'exécutant (volet négatif de la partialité) et la capacité de l'exécutant à produire des PE supplémentaires (volet positif de la partialité).

Ensuite, pour revenir aux PN, on a vu que leurs formats dont l'identité est exigée par la loi de la neutralité exécutive portent sur des *opérations* : une suite binaire formalise une production de données ; une instruction machine formalise des opérations arithmétiques, comparatives, logiques ou de transfert ; un datagramme formalise l'émission d'une requête etc. Les opérations numériques ainsi formalisées, l'identité entre leurs formats entraîne celle entre ces opérations elles-mêmes. L'exigence d'une identité formelle (loi de la neutralité) peut alors être complétée par une exigence d'identité opérationnelle (loi de l'interopérabilité). En découle une **loi de l'interopérabilité exécutive** en vertu de laquelle **l'exécution d'une PN n'autorise pas d'écart opérationnel**. À nouveau, l'anéantissement d'un tel écart empêche l'appréciation exécutive d'intervenir dans la validation de la PN et de potentiellement détourner l'identité entre les opérations. Ainsi lié par des opérations, on a souligné que l'exécutant est aliéné par l'une d'entre elles en particulier – la sollicitation (requête d'accès), concentratrice des formats appelés à être identiques. Sur ces observations, la loi de l'interopérabilité exécutive implique à la fois l'intégrité de la PN malgré la multitude d'opérations numériques qu'elle rencontre (exécutions, interférences potentielles de PN tierces...) et l'aliénation de l'exécutant à la sollicitation. On a vu aussi que l'interopérabilité pose une exigence de cohérence mathématique entre la PN dont l'exécution est requise et les autres PN stockées par la machine. Inversement, une telle loi est impraticable pour la validation de prescriptions étatiques. L'absence d'identité opérationnelle oblige l'exécutant à évaluer la correspondance entre des opérations concrètes (par ex., faits concernés dans un cas concret) et des règles abstraites (par ex., énoncé du F d'une règle invoquée), puis entre des règles abstraites (par ex., énoncé du C d'une règle invoquée) et des opérations concrètes (par ex., sanction prononcée par l'exécutant dans le cas concret). Cumulée avec la loi de la partialité exécutive,

cette évaluation se fait à coup d'appréciations par lesquelles l'exécutant prête une nouvelle signification à la PE exécutée. En l'absence d'identité opérationnelle, l'exécutant d'une PE est donc régi par une loi de l'interprétation exécutive qui implique à la fois l'impossibilité pour la PE de conserver son intégrité face aux correspondances opérations-règles évaluées par l'exécutant (volet négatif de l'interprétation) et la souveraineté de l'exécutant pour signifier ces correspondances (volet positif de l'interprétation).

Enfin, on a vu que l'application d'une PN est solidaire de son exécution : le processeur applique la PN qu'il exécute sans le moindre écart formel, opérationnel ou même temporel pour séparer ces deux actions. S'en infère une troisième **loi de la solidarité applicative** en vertu de laquelle **l'application d'une PN n'autorise pas d'écart avec son exécution**. À nouveau, l'anéantissement d'un tel écart empêche toute appréciation applicative de dévier le résultat de l'exécution. Ainsi lié par le résultat de l'exécution, l'applicateur est privé du pouvoir de produire des PN supplémentaires. Surtout, l'exécution étant solidaire de l'application, l'opération par laquelle est ordonnée l'application concrète d'une PN peut précéder cette exécution par la même occasion qu'elle précède l'application ; l'applicateur est lié par un ordre concret d'application formulé non à l'étape de l'exécution mais à l'étape antérieure de la sollicitation (requête d'accès). La loi de la neutralité applicative implique à la fois l'intégrité de l'application de la PN face à un applicateur privé de tout pouvoir d'appréciation et de création de PN supplémentaires (volet positif de la solidarité) et l'aliénation de l'exécutant-applicateur à l'ordre d'application formulé par la sollicitation (volet négatif de la solidarité). Inversement, une telle loi est impraticable pour l'application de prescriptions étatiques, où l'exécution est en principe séparée formellement, opérationnellement et temporellement de l'application. Certes, on a constaté dans la modélisation complexe d'une PE que, en menant un travail de validation, l'applicateur d'une PE fait acte d'exécution. Cependant, d'une part, ce travail d'exécution n'étant régi ni par la neutralité ni par l'interopérabilité exécutives, la confusion de l'applicateur et de l'exécutant en une même personne n'engendre pas de soumission de l'applicateur étatique à ces lois. D'autre part, l'application d'une PE étant nécessairement précédée par au moins une exécution qui lui est distincte, l'étape directement antérieure à l'application réside dans l'exécution et non dans la sollicitation ; l'ordre concret d'application de la PE auquel est lié l'applicateur n'est donc pas formulé par la sollicitation mais par l'exécutant lui-même, conduisant cet applicateur à appliquer la PE transmise par l'exécutant tout en étant délivré de celle invoquée par la sollicitation. En complément des lois de la partialité et de l'interprétation exécutives, l'applicateur étatique également exécutant obéit à une loi d'autonomie applicative qui implique à la fois l'impossibilité pour la PE d'être appliquée de manière intègre face aux appréciations d'un exécutant-applicateur régi par les lois de partialité et d'interprétation exécutive (volet négatif de l'autonomie) et la liberté de l'applicateur à l'égard de la sollicitation originelle (volet positif de l'autonomie).

On tire deux observations principales de cette comparaison entre PE et PN. **Premièrement, la réalisation d'une prescription est régie par des lois propres** : inexistantes voire impraticables pour d'autres types de prescriptions tels les PE, les lois de neutralité et d'interopérabilité exécutives et la loi de solidarité applicatives sont propres à la réalisation d'une PN ; inversement et pour les mêmes raisons, les PE sont régies par leurs lois propres de réalisation. On en conclut que **la machine numérique renferme une activité prescriptive interne régie par des lois propres**. Sans nécessairement être pourvues d'intelligence au sens humain de la chose, les machines font preuve d'une compréhension mutuelle gouvernée par des lois internes afin d'aboutir à la réalisation de prescriptions. **Deuxièmement, l'effectivité d'une**

prescription est modulée par les lois propres de sa réalisation : comme on l'a expérimenté *supra*, les lois propres à la réalisation d'une PN abstraite lui garantissent une effectivité concrète intègre, totale et absolue, tandis que les lois propres à la réalisation d'une PE (partialité et interprétation exécutives, autonomie applicative) contraignent son effectivité concrète à être déviée, partielle et relative. On confirme alors que deux prescriptions (par ex. une issue d'une activité sociale-humaine, l'autre de l'activité numérique interne) ne produisent pas les mêmes effets selon les lois grâce auxquelles elles s'épanouissent, et qu'elles sont donc dissemblables dans leur effectivité. Dans le cas de la PN, son effectivité est encore modulée lorsqu'elle est diffusée en ligne car de nouvelles lois internes s'ajoutent à celles étudiées.

B) Lois internes imputables à la structure numérique en réseau de machines connectées (« lois internes au réseau »)

Structurées par les propriétés fonctionnelles d'une machine-hôte, les lois de neutralité et d'interopérabilité exécutives et la loi de solidarité applicative appartiennent à une structure numérique locale. Diffusée en ligne, la PN dépasse toutefois le seul champ local d'une machine-hôte et intègre en plus celui de machines en réseau dont la propriété fonctionnelle d'être interconnectées structurent de nouvelles lois internes à l'activité numérique. Toute PN *en ligne* emprunte donc deux structures numériques qui se superposent, l'une locale l'autre en réseau, chacune agencée par ses propres activités, lois et fonctionnements. Or, les lois de réalisation d'une prescription faisant varier son effectivité, l'emprunt d'une structure supplémentaire par la PN *en ligne* équipe cette dernière d'une effectivité nouvelle par rapport à la PN *hors ligne*. L'effectivité de la PN en ligne demeure intègre, totale et absolue puisque, les structures locale et en réseau étant superposées sans se contredire, cette PN demeure régie par les lois internes locales. Le changement apporté à l'effectivité de la PN par les lois internes au réseau se situe plutôt dans l'échelle de cette effectivité : cette échelle n'est plus cantonnée à une seule machine isolée, mais étendue à une multitude de machines connectées. **La structure numérique en réseau offre ainsi à n'importe quelle PN de déployer son effectivité** (intègre, totale, absolue) **à l'échelle de ce réseau**, potentiellement mondial comme c'est le cas d'internet.

Cette variation de l'effectivité de la PN dépend donc de l'obéissance des machines connectées à une interconnexion numérique qui se décline sous trois modalités. D'abord, ces machines obéissent à une **loi d'interconnexion binaire** en vertu de laquelle **des machines connectées doivent être mutuellement capables de comprendre le langage dans lequel une PN est énoncée**. On sait que, au contraire du format analogique accusé par différents ordres de mesures (°C/F/K pour la température, seconde/minute/heure pour le temps, décibels pour l'acoustique etc.), le format numérique ne propose qu'un seul ordre de mesure universel (binaire) [*supra*] ; en tant qu'elle est binairement formulée, une PN est alors universellement mesurable (donc compréhensible) par toutes les machines numériques connectées. Quant aux implications pour les machines, cette interconnexion binaire est source d'une **numérisation universelle** : toute machine doit être numérisée pour être connectée à un réseau numérique. Quant aux implications pour les prescriptions, l'interconnexion binaire façonne une **compréhension universelle des PN** : toute PN est binairement compréhensible à l'échelle d'un réseau numérique entier. Ces deux implications combinées, n'importe quelle PN diffusée sur un réseau numérique peut être à la fois comprise par et produite depuis n'importe quelle machine numérique connectée à ce réseau.

Ensuite, ces machines obéissent à une **loi d'interconnexion protocolaire** en vertu de laquelle **des machines connectées doivent être capables de se reconnaître mutuellement**. En suivant les mêmes protocoles logiciels (Ethernet, TCP, IP...), les machines peuvent s'identifier comme appartenant aux mêmes réseaux (Ethernet, Internet...) et en déduire leur interconnexion. Quant aux implications pour les machines, cette interconnexion de nature logicielle *via* des protocoles réseau provoque une **équidistance** à son tour **logicielle entre les machines membres d'un même réseau** : chaque membre du réseau se situe à égale distance logicielle de chaque autre membre du réseau – ou, pour le dire autrement, le concept de « distance géométrique » ne contraint pas l'interconnexion protocolaire de machines. Quant aux implications pour les prescriptions, l'interconnexion protocolaire engendre une **disponibilité irréductible des PN en ligne** : une PN (publication sur un site web, enregistrement d'un document texte, téléchargement de fichiers vidéos...) mémorisée sur une machine connectée au réseau (un serveur, un périphérique comme une clé USB, un terminal...) est, du fait de cette mémorisation, nécessairement disponible d'accès sur ce réseau à toute autre machine connectée par les mêmes protocoles⁴¹².

Enfin, ces machines obéissent à une **loi d'interconnexion opérationnelle** en vertu de laquelle **des machines connectées doivent être mutuellement capables d'exécuter une PN**. Comme on l'a remarqué en étudiant la modélisation complexe, l'interopérabilité à l'échelle d'un réseau numérique a pour effet de mutualiser l'exécution d'une PN. L'exécution d'une même PN en ligne fait l'objet d'une multitude de validations qui s'insèrent entre la production et l'application de cette PN, et qui engendrent des interférences de cette PN avec des PN supplémentaires. Quant aux implications pour les machines, cette interconnexion opérationnelle fonde une **interdépendance des exécutants connectés au même réseau numérique** : toute opération de validation par un exécutant connecté au réseau est liée par la validation de l'exécutant antérieur. Quant aux implications pour les prescriptions, l'interconnexion opérationnelle induit une **interactivité des PN présentes sur un même réseau** (*i.e.* mémorisées sur au moins une des machines connectées à ce réseau) : les interférences de PN concrétisées par les opérations interconnectées d'exécution sont génératrices d'une activité prescriptive interne au réseau, connue et comprise des seules machines connectées. Ces deux implications combinées, l'exécutant neutre et aliéné d'une PN se contente de valider des interférences prescriptives (entre PN-1 et PN-2, PN-2 et PN-3...) sans s'y ingérer, stimulant par-là une interactivité prescriptive qui le dépasse.

On explorera dans le chapitre suivant le rôle de ces trois lois sur l'activité prescriptive interne au réseau, mais on peut d'ores et déjà relever que **chacune de leurs six implications identifiées amplifie d'autant l'effectivité d'une PN**. Encadrée par les lois internes au réseau, l'effectivité d'une PN acquiert de nouvelles propriétés. La loi d'interconnexion binaire apporte ainsi à la PN une **effectivité universelle** : la qualité « numérique » d'une machine connectée suffit à rendre possibles la production, l'exécution et l'application d'une PN en quelque endroit du réseau auquel cette machine est connectée, *i.e.* auprès de n'importe laquelle des autres machines connectées à ce réseau numérique (numérisation universelle). Ainsi, contrairement à une

⁴¹² Certains protocoles (par ex. ceux régissant les pare-feu chinois) ou certaines techniques (par ex., blocage d'une adresse IP depuis les routeurs) peuvent certes rendre plus difficile l'accès effectif à une PN, mais cette PN n'en demeure pas moins disponible d'accès depuis le réseau internet (par ex. en téléchargeant des VPN locaux pour contourner un opérateur chinois, ou en empruntant une autre adresse IP – distribuée par un logiciel consacré, localement modifiée par hack, héritée de l'utilisation d'un nouveau terminal, exploitée par cyberattaque...) du moment qu'elle est mémorisée par une machine connectée à ce réseau.

PN hors ligne dont la présence locale circonscrit son potentiel d'exécution et d'application à la machine-hôte, la présence d'une PN sur un réseau numérique lui procure la capacité d'étendre son exécutabilité et son applicabilité à n'importe quelle machine numérique connectée à ce réseau (compréhension universelle des PN). Les effets d'une règle numérique $F \rightarrow C$ auprès d'un exécutant et d'un applicateur concrets sont ici une première fois amplifiés par la possibilité, pour toute machine connectée au réseau, d'exécuter-appliquer une PN présente sur ce réseau.

Par rapport à la PN hors ligne, la loi d'interconnexion protocolaire enrichit quant à elle la PN en ligne d'une **effectivité par l'accès** : cette interconnexion ne souffrant pas la distance géographique, toute machine connectée au même réseau peut accéder logiquement à une PN – *i.e.* en solliciter l'exécution – dont la présence binaire sur ce réseau lui garantit d'y être exécutable et applicable à tout moment (équidistance logicielle entre les machines). Ainsi, se tenant toujours à disposition d'une demande valide d'exécution, une PN présente sur un réseau étend son exécution et son application concrètes chaque fois qu'y accède une machine connectée à ce réseau (disponibilité irréductible d'une PN). Les effets d'une règle numérique $F \rightarrow C$ auprès d'un exécutant et d'un applicateur concrets sont une deuxième fois amplifiés par la possibilité, pour toute PN présente en ligne, de voir continuellement augmenter ou diminuer le nombre de ses exécutions-applications au rythme des accès qui y sont faits.

Pour terminer, la loi d'interconnexion opérationnelle confère à la PN en ligne une **effectivité inter-prescriptive** : l'exécution d'une PN en ligne résulte d'une sollicitation valide, émise par l'exécutant antérieur à l'issue de la validation d'une autre PN ; une sollicitation valide offre donc à ces deux PN d'interférer, et à cette interférence d'être concrétisée opérationnellement sans que soit altérée l'intégrité respective de ces PN (interdépendance des exécutants interconnectés). Ainsi, au moyen de leur interférence opérationnelle, deux PN étendent réciproquement leur exécution-application sans que cette extension réciproque de leurs effets soit modifiable par l'exécutant récepteur d'une sollicitation valide (interactivité des PN). Les effets d'une règle numérique $F \rightarrow C$ auprès d'un exécutant et d'un applicateur concrets sont une troisième fois amplifiés par la possibilité, pour des PN interférant en ligne, de s'échanger une effectivité inter-prescriptive hors du contrôle de l'exécutant-applicateur et tributaire d'une sollicitation valide.

Comme on l'a noté pour les PE et les PN hors ligne, l'effectivité de la PN en ligne est modulée (ici triplement amplifiée) par les lois propres à sa réalisation sur un réseau numérique (interconnexions binaire, protocolaire, opérationnelle). Par sa diffusion en ligne, la PN déploie les nouveaux effets que lui confèrent ces lois internes au réseau, et stimule ainsi une nouvelle activité (*i.e.* un nouveau procédé d'actions) tout aussi interne au réseau numérique : de l'énonciation d'une règle numérique jusqu'à son application, le procédé d'actions compris et impulsé par les machines connectées pour la réalisation d'une PN en ligne admet ainsi pour nouveautés l'exécutabilité et l'applicabilité universelles d'une PN, l'interdépendance exécutive de toutes les machines connectées ou encore l'interactivité prescriptive par laquelle toute PN peut enrichir réciproquement son effectivité (autant de réactions machinales interconnectées que n'admet pas le procédé d'actions d'une machine-hôte locale pour la réalisation d'une PN hors ligne).

On peut dès lors **apporter confirmation à la première hypothèse** faite *supra* selon laquelle, **comme la matière physique comporte des lois propres régissant son activité atomique interne distinctement de celles régissant son utilisation humaine externe, la machine numérique connectée comporte des lois régissant son activité prescriptive interne distinctement de celles régissant son utilisation humaine externe**. Pour le cas de l'atome, on

a par ailleurs observé que l'utilisation externe d'un objet physique n'est pas imperméable aux lois atomiques : en en modifiant l'utilisabilité, ces lois modifient les rapports de force interhumains nés de l'utilisation de cet objet. Reste en retour à savoir si les rapports de force interhumains nés de l'utilisation d'une machine numérique connectée sont également perméables aux lois numériques identifiées.

Paragraphe 2 – L'influence des lois numériques internes sur les rapports de force interhumains

Les lois qu'on a extraites de l'activité numérique interne instaurent un mode prescriptif qui, en façonnant les modalités pour prescrire sur un réseau numérique (A), sculpte des compétences humaines sources de rapports de force interhumains en ligne (B)

A) Mode prescriptif numérique et pouvoir de prescrire en ligne

Notre intérêt pour les lois internes dans l'étude des rapports de force interhumains réside précisément dans la vérification de cette seconde hypothèse : comment les lois internes au réseau numérique, en paramétrant les capacités humaines d'utilisation d'un tel réseau, influencent-elles ces rapports de force ? Comment, à partir de ses lois internes, le réseau numérique décuple-t-il l'aptitude humaine à imposer des actes et décisions en société ?

En approfondissant la donnée en ligne telle que comprise par les machines connectées, notre étude endogène du réseau numérique nous a fait constater que les lois internes à ce réseau établissent un pouvoir de caractère prescriptif. Auprès de la société humaine, cette particularité prescriptive endogène de la donnée binaire en ligne a donc pour répercussion essentielle de confier à l'être humain le pouvoir d'imposer un nouveau type de prescriptions – des prescriptions « numériques » en réseau. Pour le dire autrement, **chaque fois qu'il diffuse en ligne des données binaire, l'être humain ordonne l'accomplissement de règles numériques exécutables et applicables par la machine numérique**. Par-là, le réseau internet accorde à l'être humain le pouvoir de produire des prescriptions, de les voir exécutées et de faire ainsi acquiescer à leurs actions numériques l'effectivité d'une PN en ligne. Ce pouvoir prescriptif en ligne de l'être humain étant sculpté par les lois internes au réseau, **c'est à ces lois qu'il convient de se référer pour connaître les conditions de production, d'exécution et d'effectivité d'une PN**.

Quant aux conditions de production, elles sont peu contraignantes pour la volonté humaine de prescrire en ligne. En posant une omniprésence du code binaire sur le réseau numérique, la loi d'interconnexion binaire démocratise et nivelle le pouvoir (humain) de produire des PN. D'une part, l'omniprésence du code binaire fait de ce code le fondement existentiel d'une PN en ligne : une donnée en ligne n'existe comme « prescription exécutable et applicable » qu'en vertu de son format binaire, sans lequel son exécutant-applicateur ne peut la comprendre comme telle. Pour produire une PN, il suffit donc de produire une donnée binaire, ouvrant par la même occasion ce pouvoir de production à la volonté de tout utilisateur d'une machine numérique connectée. Ces conditions de production d'une PN ouvertes à la volonté humaine rompent radicalement avec celles d'une prescription étatique (PE), fermées à une telle volonté – les acteurs capables d'en produire le sont par habilitation étatique, ce qui rend le désir d'en produire très largement insuffisant pour en produire concrètement. D'autre part, l'omniprésence du code binaire fait de ce code l'élément de composition de toute PN en ligne : les PN sont exécutées-appliquées en vertu d'un format binaire qu'elles partagent toutes en commun,

universellement déclencheur de leur concrétisation. Toute PN se produit donc de la même manière, *i.e.* par la génération de données binaires, égalisant par-là les prescripteurs humains dans leur capacité à produire des PN. Ces conditions égalitaires de production d'une PN en ligne se démarquent à nouveau de celles statutaires d'une PE – la manière de produire une PE n'est pas figée par un format exclusivement et universellement reconnu valide, mais varie selon les statuts diversement reconnus par l'État aux prescripteurs (juge, législateur, administration...).

Ainsi, le **pouvoir ouvert et égalitaire de produire des PN** autorise tout utilisateur (humain) à produire une PN et à le faire uniformément ; en conséquence, toute volonté humaine et une même volonté humaine peut prescrire numériquement en qualité, tour à tour, d'internaute, de développeur ou encore de hacker. *A contrario*, le pouvoir fermé et statutaire de produire des PE restreint le champ des prescripteurs aux seuls acteurs (humains) habilités par l'État ; en conséquence, il est impossible à l'ensemble des volontés humaines de produire des PE en qualité alternativement de législateur, de juge et d'autorité administrative.

Quant aux conditions de concrétisation (exécution-application) de la PN, elles préservent la demande humaine fidèlement à son énonciation numérique. Cette fois régi par les lois internes locales (neutralité et interopérabilité exécutives, solidarité applicative), le pouvoir qu'a l'être humain de voir exécutées les PN qu'il a produites est doublement caractérisé par une abstention et par une subordination de l'exécutant-applicateur. D'une part, on a vu que ces lois ont pour première implication commune d'obliger l'exécutant-applicateur à conserver l'intégrité de la PN produite lors de sa validation : tant la neutralité et l'interopérabilité exécutives que la solidarité applicative font obstacle à la survenance d'un écart interprétatif, rendant du même coup l'exécutant-applicateur indifférent au contenu de la PN (*i.e.* aux éléments qui composent son F et son C) lorsqu'il en valide le format. Cette indifférence garantit la concrétisation intacte du contenu de la règle numérique telle que la demande l'être humain producteur de données. La demande humaine est inaltérée par rapport à sa concrétisation. Si les conditions pour concrétiser une PN sauvent la demande humaine de toute altération, on sait qu'il en va différemment de la demande humaine de concrétiser une PE, dévoyée d'ici à son accomplissement – sous le coup des lois de partialité et d'interprétation exécutives et de la loi d'autonomie applicative, le contenu de la PE appliquée diverge du contenu de la règle dont la concrétisation est demandée. D'autre part, on a vu que les lois locales internes au réseau numérique ont pour seconde implication commune de subordonner l'exécutant-applicateur à la validité de la sollicitation l'appelant à concrétiser une PN (requête d'accès) : on sait que cette sollicitation concentre les formats devant être validés comme identiques aux formats déjà reconnus valides par l'exécutant-applicateur neutre. À ce titre, la concrétisation de la PN dépend non de la liberté d'appréciation de cet exécutant-applicateur mais d'une sollicitation dont la validité (*i.e.* l'identité avec des formats valides) antérieure à l'exécution emporte validation de la règle demandée à être concrétisée. Exprimée à travers une sollicitation numérique, la demande humaine aliène la concrétisation de la PN. En opposition, loin d'être aliénée par la demande humaine d'exécution, la concrétisation d'une PE n'est de son côté guère contrainte par une telle demande – au moyen de leur appréciation, l'exécutant et l'applicateur se réapproprient la concrétisation de la PE demandée en y substituant la PE qu'ils produisent.

Ainsi, le **pouvoir inaltéré et aliénant de voir concrétisée une PN** assure à l'utilisateur (humain) qui la demande d'obtenir la concrétisation intègre d'une PN et d'obliger l'exécutant-applicateur à une telle concrétisation ; en conséquence, l'absence de biais entre la demande humaine et la concrétisation de la PN inclut cette demande humaine parmi la communauté des

prescripteurs numériques (en qualité de créateurs de prescriptions concrètes) et en exclut l'exécutant-applicateur (aliéné, privé du pouvoir de produire des PN). *A contrario*, le pouvoir dévoyé et non-contraignant de voir concrétisée une PE n'octroie pas à l'être humain le pouvoir d'obliger l'exécution et l'application demandées à conserver l'intégrité de la PE, dont la concrétisation est réappropriée par l'exécutant et l'applicateur ; en conséquence, la substitution de la PE demandée par celle concrétisée exclut cette demande humaine de la communauté des prescripteurs étatiques (non-contraignante, privée du pouvoir de produire des PE), et y inclut l'exécutant et l'applicateur (en qualité de créateur de PE abstraites et concrètes).

Quant aux conditions d'effectivité de la PN en ligne, elles grossissent considérablement l'action humaine. Cet accroissement est dû aux lois d'interconnexion protocolaire et opérationnelle qui fournissent respectivement à la PN une portée ubiquitaire et une portée ordonnatrice. D'une part, en rendant la PN présente en ligne constamment accessible à l'échelle d'un réseau entier (disponibilité irréductible), la loi d'interconnexion protocolaire dote chaque PN d'une égale portée ubiquitaire. N'importe quelle PN en ligne peut étendre ses effets auprès d'un exécutant-applicateur connecté au réseau. Accessible à quiconque est connecté au même réseau, toute action numérique de l'utilisateur (humain) devient une prescription dont l'effectivité s'agrandit à mesure des accès. D'autre part, en occasionnant des interférences de PN (interactivité des PN), la loi d'interconnexion opérationnelle fait s'articuler les PN dans un « ordonnancement », *i.e.* un ensemble rendu cohérent par les interactions qu'il renferme⁴¹³. La portée (ordonnatrice) acquise par la PN au sein de cet ordonnancement équivaut donc à l'étendue de ses effets acquis par interférences avec d'autres PN auprès de nouveaux exécutants-applicateurs connectés. Plus l'interactivité d'une PN en ligne avec les autres augmente, plus s'étend son effectivité auprès des machines connectées à un même réseau, plus elle représente une part importante des interférences qui ordonnancent ce réseau. En s'insérant dans un ordonnancement, l'effectivité de l'action humaine en ligne obéit aux lois de cet ordonnancement qu'on examinera dans le Chapitre suivant.

Pour distinguer clairement les interactions de PN dans le cyberspace, il faut différencier les PN et les données qui découlent de leur application. Prenons l'exemple de Bob qui utilise sur son smartphone l'application mobile Le Monde pour publier en ligne le commentaire « *les arabes remplacent les français* ». Dans ce cas, l'application mobile Le Monde est le client grâce auquel Bob accède au service en ligne Le Monde. En premier lieu, le smartphone depuis lequel Bob rédige son commentaire fait interagir plusieurs prescriptions numériques : celles qui ordonnent au processeur d'exécuter les adresses mémoire des instructions impliquées par la requête de Bob ; celles qui puisent dans la table des caractères pour ordonner au processeur du smartphone d'exécuter le message ; celles qui ordonnent au processeur d'exécuter le « clic » de Bob sur le bouton « publication du commentaire » proposé par l'application mobile ; celles qui ordonnent au processeur de traiter en priorité la requête de Bob par rapport aux autres processus en cours (interruptions) ; celles qui ordonnent au processeur de communiquer avec la carte réseau du smartphone pour transmettre les données sur le réseau ; celles de l'application mobile qui permettent de communiquer la requête de Bob aux serveurs du Monde... Toutes ces PN

⁴¹³ L'ordonnancement est une partie d'un concept plus large qu'on examinera plus loin - le système. On appelle « système » tout ensemble organisé par les échanges de ses composants entre eux *et avec le milieu extérieur*. On appelle « ordonnancement » la partie du système qui est organisée par les échanges de ses composants *entre eux* uniquement, c'est-à-dire par les échanges internes au système uniquement sans y inclure les échanges avec l'environnement extérieur au système.

interagissent localement à travers leur exécution par le processeur du smartphone de Bob. En deuxième lieu, parmi ces PN locales, seules celles communiquées par le client (application mobile Le Monde) à destination du serveur hébergeant Le Monde interagissent avec les PN locales stockées par ce serveur - c'est le fameux « environnement client-serveur ».

En troisième lieu, après que le serveur du Monde ait exécuté la requête de Bob, il ne stocke plus cette requête ; il stocke seulement les données dont la requête ordonnait la publication, c'est-à-dire le commentaire de Bob. En d'autres termes, les données stockées sur le serveur ne sont pas ici des prescriptions numériques car le message de Bob n'est plus assorti d'instructions - ces dernières ont toutes été exécutées. Ne restent stockées sur le serveur du Monde que les données de caractères constitutives du message de Bob. Enfin, si un utilisateur tiers accède au commentaire de Bob hébergé par le serveur du Monde, les PN produites par cet utilisateur tiers n'interagissent pas avec celles produites par Bob : cet utilisateur tiers ne fait qu'accéder à des données de caractère non porteuses de PN même si, pour y accéder, il doit faire interagir ses PN locales avec celles stockées par le serveur du Monde et par les routeurs qu'il emprunte. Par conséquent, il importe de différencier l'échelle de diffusion d'une donnée (le commentaire publié par Bob) et la portée ordonnatrice d'une PN (la requête de Bob). Le commentaire publié par Bob est stockée par trois machines différentes, et son échelle de diffusion s'étend donc à ces trois machines (le terminal de Bob, le serveur du Monde et le terminal de l'utilisateur tiers qui y accède). En revanche, la requête de Bob n'a pas contraint le terminal de l'utilisateur tiers, et les PN produites par Bob n'ont pas interagi avec celles produites par l'utilisateur tiers ; la portée ordonnatrice de cette requête est donc plus limitée que l'échelle de diffusion du commentaire publié par Bob. Cependant, **c'est bien grâce à sa portée ordonnatrice qu'une PN peut provoquer le stockage de données qui acquerront une échelle de diffusion dans le cyberspace** : si les PN émises par Bob n'avaient pas contraint le smartphone de Bob, les routeurs empruntés et le serveur du Monde à exécuter la requête de Bob, son commentaire n'aurait pas pu être publié en ligne, et n'aurait donc pas pu obtenir d'échelle de diffusion dans le cyberspace. L'échelle de diffusion d'une donnée (ici le commentaire de Bob) est donc alimentée par les portées ordonnatrices des différentes PN stockées et produites en ligne. On dira alors du mode d'ordonnement des PN qu'il est à la fois ubiquitaire (il permet les interactions de PN quel que soit le « lieu » où sont stockées ces PN) et diffusible (les données dont une prescription numérique ordonne le stockage peuvent gagner une échelle de diffusion auprès des autres processeurs exécutants membres du réseau).

En somme, le **pouvoir ubiquitaire et diffusible de prescrire en ligne** alloue à la PN dont l'utilisateur (humain) est l'auteur la capacité d'être constamment accessible et tout aussi constamment d'élargir son effectivité par l'échelle de diffusion qu'acquièrent les données issues de l'exécution de cette PN. La portée ordonnatrice d'une PN (interne au réseau) constitue la base des rapports de force interhumains (externes au réseau) qui naissent des données diffusées sur internet, pour minimiser ou maximiser les effets numériques d'une action humaine selon l'échelle de diffusion acquise par ces données dans le cyberspace. À la différence des comparaisons précédentes avec le pouvoir prescriptif étatique, on retrouve ces deux propriétés ubiquitaire et diffusible dans les conditions d'effectivité de la PE – déployant ses effets par ses interactions avec d'autres PE au sein d'un même ensemble prescriptif étatique cohérent (donc ordonnatrice de cet ensemble), grâce à sa constante disponibilité d'exécution dans un ordre juridique quel qu'ait été l'auteur ou le lieu de son édicton (donc ubiquitaire dans cet ordre) et grâce aux décisions et raisonnements sur lesquels elle débouche, qui peuvent être repris et gagner une échelle de diffusion auprès des autres exécutants membre de cet ordre juridique (donc diffusible dans cet ordre). Ce point commun entre PE et PN ne fait pas pour autant sauter toute disparité sur

le terrain de leur effectivité. À ce titre, comme on l'a déjà démontré, l'effectivité fournie à la PN par sa portée ordonnatrice et sa portée ubiquitaire bénéficie également à toute volonté humaine (conditions de production de la PN) et contraint l'exécutant-applicateur à préserver l'intégrité de toute demande humaine de concrétisation (conditions de réalisation de la PN), tandis que l'effectivité de la PE acquise par ses portées ordonnatrice et ubiquitaire relève statutairement de quelques volontés humaines (conditions de production de la PE) et résulte d'une déviation de la demande humaine de concrétisation par l'exécutant et l'applicateur qui y substituent d'autres PE (conditions de réalisation de la PE).

On en conclut que, en assignant à l'être humain des capacités de prescrire en ligne distinctes de ses capacités de prescrire au moyen de l'État, les six lois identifiées comme internes à la machine numérique connectée déterminent l'utilisabilité humaine de cette machine, qu'on a précédemment définie comme « *les pouvoirs techniques accordés à l'utilisateur humain* ». En ce sens, on confirme que cette utilisabilité de la machine fait le pont entre ses lois internes et les pouvoirs humains externes. On a dans ce cadre dénombré six retentissements de l'interne sur l'externe : les lois internes relevées établissent l'existence de pouvoirs de production prescriptive (i) ouvert et (ii) égalitaire au bénéfice de la volonté humaine, de concrétisation prescriptive (iii) inaltéré et (iv) aliénant au bénéfice de la demande humaine, d'effectivité prescriptive (v) ubiquitaire et (vi) diffusible au bénéfice de l'action humaine. Afin d'en faciliter la compréhension, on rangera dans un « mode prescriptif numérique en ligne » les lois internes locales et en réseau relevées telles qu'elles définissent les conditions de réalisation d'une PN et les retentissements de ces conditions auprès des capacités humaines de prescription. Ainsi dira-t-on du **mode prescriptif numérique en ligne** qu'il est composé d'un mode de production **ouvert et égalitaire**, d'un mode de concrétisation **inaltéré et aliénant** et d'un mode d'effectivité **ubiquitaire et diffusible** – dissemblable au **mode prescriptif étatique fermé et statutaire** (à l'égard de la volonté humaine), **dévoyé et affranchi** (à l'égard de la demande humaine), **ubiquitaire et diffusible** (à l'égard de l'action humaine).

En raison d'une telle détermination du pouvoir humain par les lois machinales internes, on retiendra ce mode prescriptif numérique comme la source de laquelle tout être humain tire son pouvoir prescriptif en ligne. De la même façon, en définissant ce pouvoir (humain) prescriptif en ligne, les caractéristiques du mode prescriptif numérique que nous venons de lister lèguent à ce pouvoir deux qualités particulières. Premièrement, le **pouvoir prescriptif en ligne** est **décentralisé** et ne peut être centralisé tant que se maintient ce mode prescriptif : l'ouverture du pouvoir de production (issue de la loi d'interconnexion binaire), l'aliénation de l'exécutant-applicateur (issue des lois locales) et la portée ordonnatrice d'une donnée en ligne (issue de la loi d'interconnexion protocolaire) reconnaissent à chaque individualité humaine l'égale capacité de produire des PN, de les voir concrétisées telles que demandées, de les insérer dans un ordonnancement d'interactions lui-même agencé par des PN venues d'une multitude dispersée d'exercices individuels du pouvoir prescriptif. La régulation du pouvoir prescriptif nécessitant de contrôler chacun de ces exercices du pouvoir individuel de prescrire en ligne, une telle régulation de ce pouvoir relève *de facto* de chaque individualité humaine apte à contrôler sa volonté, sa demande et son action en ligne. À l'opposé, le pouvoir prescriptif étatique est centralisé : la fermeture du pouvoir de production, l'affranchissement de l'exécutant et de l'applicateur à l'égard de la demande humaine et la portée ordonnatrice d'une règle de droit réservent à l'État et aux acteurs qu'il habilite la capacité de produire des PE, de les concrétiser souverainement, d'en faire fluctuer l'effectivité ordonnatrice. La régulation du pouvoir prescriptif étatique relève donc d'un État central, distributeur, définisseur et contrôleur de ce pouvoir dont il est titulaire.

Deuxièmement, le **pouvoir prescriptif en ligne** est **horizontal** : l'égalité du pouvoir de production (issue de la loi d'interconnexion binaire), l'indifférence de l'exécutant-applicateur (issue des lois locales) et la portée ubiquitaire d'une donnée en ligne (issue de la loi d'interconnexion protocolaire) effacent toute distinction hiérarchique entre les PN selon leur provenance, leur format, leur contenu ou leur accessibilité. Dans ces conditions, une régulation des PN en ligne qui s'appuie sur ces quatre derniers critères (filtrage des formats par *deep packet inspection*, illicéité d'un contenu publié, blocage de l'accès à une donnée en ligne...) ne régule que les utilisations humaines de la machine connectée et non le mode prescriptif numérique auquel chaque utilisateur doit son pouvoir prescriptif. Dès lors, une telle régulation laisse entière l'horizontalité décrite du pouvoir prescriptif en ligne. À l'opposé, le pouvoir prescriptif étatique est vertical : le pouvoir statutaire de production, la dérivation de la demande humaine de concrétisation par l'exécutant et par l'applicateur habilités, et la portée ubiquitaire d'une règle de droit assurent aux PE de surplomber les volontés et demandes humaines de concrétisation en étant exclusivement produites par l'État, dont l'organisation statutaire lui fait distinguer les PE selon leurs statuts formels (rang normatif de la PE, acteur duquel provient la PE, procédure d'édiction de la PE...) souverainement reconnus par l'État ou selon leurs contenus matériels (valeur morale/politique/sociale de ce contenu, répercussions de ce contenu, force matricielle de ce contenu dans l'ordre juridique...) tout aussi souverainement appréciés par l'exécutant et l'applicateur étatiques, habilités eux-aussi par statut. En vertu de cette verticalité, la régulation du mode prescriptif étatique n'appartient une fois de plus à personne d'autre qu'à l'État lui-même, la verticalité du pouvoir prescriptif étatique étant ainsi complémentaire de sa centralité.

En somme, on peut théoriquement confirmer que, par l'intermédiaire de l'utilisabilité, les lois régissant l'activité interne de la machine connectée déterminent les pouvoirs techniques externes de l'être humain, et que ces pouvoirs ainsi déterminés ne peuvent en eux-mêmes être régulés de manière verticale ou centralisée. Tant que la régulation ne change pas les lois internes identifiées (neutralité et interopérabilité exécutives, solidarité applicative, interconnexions binaire, protocolaire et opérationnelle), les caractéristiques du mode prescriptif en ligne qui en découlent restent pareillement inchangées (ouvert, égalitaire, inaltéré, aliénant, ubiquitaire et diffusible), tout comme les qualités du pouvoir prescriptif en ligne (décentralisé/horizontal). Avant de tenir le pouvoir prescriptif en ligne pour le point de jonction entre l'activité interne de la machine connectée et la régulation des rapports de force interhumains en ligne, reste à savoir si ce pouvoir suscite en pratique de tels rapports de force.

B) Mode prescriptif numérique et rapports de force interhumains en ligne

On a dit du pouvoir de l'internaute qu'il demeurerait un mystère pour les explications endogènes des rapports de force en ligne. Les explications virtualiste (D. Post et D. Johnson), partiellement endogènes (Y. Benkler et J. Boyle) et CodIL étudiées – en partant des caractéristiques qu'elles identifient comme internes au réseau (immatérialité de l'accès logiciel aux informations en ligne, informations non rivales et non excluables, détermination par le code source des capacités logicielles d'action) – ne permettent de déceler chez l'internaute qu'un pouvoir endogène respectivement d'accès logiciel, d'utilisation valorisante de l'information, et d'utilisation non contraignante d'un logiciel lui seul contraignant. La capacité de l'internaute, illustrée par le cas JVC, à « gagner » un rapport de force l'opposant au gestionnaire d'un logiciel ne peut dès lors trouver auprès de ces auteurs qu'une explication exogène, tels que la force de la communication humaine en ligne, l'exploitation économique collective d'un espace informationnel ou encore la plus traditionnelle normativité sociale.

Après avoir étudié la compréhension de l'action humaine par la machine connectée, **nous obtenons une autre conclusion endogène** établissant que, le pouvoir légué à l'internaute par les caractéristiques internes de la machine connectée étant un pouvoir à caractère prescriptif, la capacité de cet internaute à gagner un rapport de force en ligne provient des prescriptions numériques binaires dont il est l'auteur. Pour aboutir à cette conclusion, on a d'abord synthétisé les résultats transcrits jusqu'ici :

Comment qualifier le pouvoir endogène de l'utilisateur ? De pouvoir prescriptif.

En quoi consiste ce pouvoir ? À ouvrir également à la volonté des utilisateurs le pouvoir de produire une prescription en produisant une donnée, d'aliéner la concrétisation de cette prescription à leur demande inaltérée, et de rendre ubiquitaire et diffusible leur action ainsi prescriptive.

Quelle effectivité apporte ce pouvoir à cette action humaine ? Une effectivité qui rend les prescriptions produites par chaque utilisateur à la fois universellement concrétisables à l'échelle d'un réseau, constamment amplifiables par les accès qui y sont faits, et réciproquement expansives par leurs interactions.

Comment s'exerce ce pouvoir ? De manière décentralisée et horizontale, la pleine et égale titularité de ce pouvoir revenant à chaque utilisateur individuellement producteur de données.

– avant d'appliquer cette synthèse au rapport de force observé dans le cas JVC. Souvenons-nous que, dans ce cas, un algorithme de modération par mots-clés (« pute », « salope » etc.) a été contourné à l'aide de caractères alphabétiques spéciaux (« pūte », « sālōpe » etc.) indétectés par le logiciel. Sans même faire l'hypothèse d'un quelconque pouvoir prescriptif, cette situation de contournement correspond-elle à un « rapport de force interhumain » tel que défini dans le cadre de cette thèse ? On rappelle avoir délimité ce concept autour de quatre critères : (i) *un type de relation interindividuelle ou de groupe par laquelle* (ii) *des êtres humains* (iii) *imposent concrètement* (iv) *leurs actes et/ou décisions à d'autres êtres humains*.

En l'espèce, (i) une communauté en ligne (ii) d'internautes (iii) oblige les serveurs hébergeant JVC et les terminaux connectés qui y accèdent (iv) à faire s'afficher au détriment de leurs propriétaires et utilisateurs humains les messages haineux publiés par cette communauté. Ce faisant, les publications haineuses s'imposent doublement au gestionnaire du logiciel et aux internautes se connectant au forum JVC, et le contournement effectué est alors constitutif d'un rapport de force. La communauté récalcitrante ne doit ainsi sa capacité d'imposer ses publications à des êtres humains – et donc ce rapport de force ne doit son existence – qu'à la capacité technique de cette communauté d'obliger des machines à concrétiser lesdites publications en les affichant. On en déduit que **ce pouvoir d'obliger la machine connectée est la cause** qui conditionne l'existence **du rapport de force interhumain en ligne**. Or, dans le cas présent, comment ce pouvoir s'exerce-t-il ? De quelle manière se forme l'obligation d'affichage pesant sur les machines connectées ? Cette obligation est technologiquement formée au moyen d'ordres, émis par la communauté récalcitrante et auxquels la machine est aliénée, d'exécuter et d'appliquer une règle issue du logiciel JVC (à savoir l'autorisation de publier de caractères alphabétiques spéciaux). Par conséquent, une telle obligation correspond à la définition éprouvée d'une prescription concrète, *i.e.* une règle dont l'exécution et l'application effectives procèdent d'un ordre d'accomplissement. Pour le dire autrement, en émettant des ordres d'accomplissement d'une règle qui en entraînent l'exécution et

l'application effective, les membres de cette communauté récalcitrante *prescrivent* la concrétisation de cette règle aux machines connectées (notamment aux serveurs de JVC, aux terminaux demandant l'accès au contenu du forum, et aux serveurs des navigateurs web exécutant ces demandes d'accès).

À partir du rapport de force interhumain identifié dans le cas d'espèce, on relève trois compétences prescriptives numériques exercées par la communauté humaine récalcitrante. Premièrement, *chacun* des membres de cette communauté est capable de prescrire la concrétisation d'une règle auprès de machines connectées, qui exécutent et appliquent cette règle *sans pouvoir s'affranchir* des ordres numériques formés par les récalcitrants *ni modifier* les contenus dont la publication est ainsi ordonnée. La compétence de produire des prescriptions étant à la fois *ouverte* à chacun de ces membres, *aliénante* pour la concrétisation et *inaltérée* par cette concrétisation, les récalcitrants peuvent obtenir une **concrétisation conforme à leur volonté et à leur demande de réaliser une règle**. Cette dernière spécificité rapproche la compétence numérique de prescrire en ligne d'un autre type de compétence prescriptive : celle de prescrire *immédiatement*, grâce à laquelle un prescripteur peut lui-même produire et concrétiser une prescription sans recourir à un intermédiaire. Mis à part ce point commun⁴¹⁴ d'une concrétisation préservatrice de la volonté et de la demande du prescripteur, le pouvoir de prescrire en ligne est loin d'être immédiat ne serait-ce que parce que les producteurs de prescriptions en ligne (communauté récalcitrante) sont dissociés des intermédiaires qui les concrétisent (machines connectées). Dès lors, ce point commun s'explique non par une identité de ces deux compétences prescriptives (numérique et immédiate), mais par la neutralité de l'intermédiaire numérique qui concrétise l'ordre prescriptif.

Deuxièmement, lorsque les membres de cette communauté publient des messages injurieux, ils le font en requérant auprès du serveur de JVC hébergeant le code source qu'il concrétise une prescription posée par le logiciel du forum (la fonctionnalité « publication de caractères alphabétiques spéciaux »). Cette prescription étant *constamment accessible* sur le réseau depuis ce serveur, sa concrétisation est non seulement permise *quelle que soit et où que se situe* la machine du récalcitrant qui l'ordonne au serveur⁴¹⁵, mais par ailleurs *amplifiée* chaque fois qu'elle est ainsi ordonnée. La compétence de faire concrétiser des prescriptions toujours *disponibles* d'accès, *ubiquitaires* et *inter-expansives* assure aux récalcitrants que **la portée de leurs demandes et de leurs volontés peut toujours être accrue par la concrétisation en ligne de ces demandes et volontés**. [C'est précisément parce que le pouvoir de prescrire est médiatisé (et non immédiat) que ces demandes et volontés peuvent ainsi être accrues]

De la même façon, en publiant des messages injurieux, les membres de cette communauté requièrent auprès d'un autre serveur de JVC, hébergeant cette fois les contenus, qu'il concrétise

414Par ailleurs relatif, car si la prescription reflète en principe la volonté du prescripteur comme c'est le cas en l'espèce, tel n'est pas toujours le cas contrairement à une compétence prescriptive immédiate. La machine connectée est certes toujours aliénée à la demande numériquement formulée par l'être humain producteur de données, mais il arrive que cette demande numérique ne corresponde pas à la volonté de cet être humain. Ainsi de l'utilisateur qui, victime d'un logiciel malveillant, effectue des actions (clic de souris, insertion de caractères...) exécutées par la machine connectée mais dont il ne maîtrise pas voire ne connaît pas les effets.

415Depuis un smartphone, ordinateur, tablette... depuis la France, les États-Unis, l'Australie... Pourvu qu'une machine est connectée au même réseau que celui sur lequel une PN est présente, cette machine peut accéder à cette PN, *i.e.* en demander l'exécution, que ladite machine soit un terminal préprogrammé avec un logiciel de censure ou qu'elle soit géographiquement située dans un pays dont les opérateurs pratiquent une censure.

les prescriptions ordonnées par les récalcitrants (les messages injurieux à publier). Tout comme la prescription posée par le logiciel (fonctionnalité de publication), celles concrètement ordonnées par les récalcitrants (contenus injurieux) sont constamment accessibles depuis le serveur JVC qui les héberge, ce quelles que soient et où que se situent les machines qui y accèdent, et sont ainsi amplifiées par les accès ordonnés auprès de ce serveur – ordres d'accès donc eux aussi constitutifs de prescriptions produites par les internautes auteurs desdits ordres. Par ces amplifications successives de la règle logicielle et des contenus, les messages injurieux prescrits par la communauté récalcitrante peuvent se diffuser dans la connaissance humaine (du gestionnaire du logiciel, des internautes accédant au forum, des annonceurs en partenariat avec ce gestionnaire...) et ainsi provoquer un rapport de force interhumain à grande échelle. On constate dès lors que, en amplifiant mutuellement leur concrétisation, les prescriptions interagissent (sur le serveur hébergeant le code source : interactions de la fonctionnalité prescrite à ce serveur par le logiciel avec les requêtes d'accès à cette fonctionnalité prescrites au même serveur par les récalcitrants / sur le serveur hébergeant les contenus : interactions des requêtes de publication de contenus prescrites à ce serveur par les récalcitrants avec les requêtes d'accès prescrite au même serveur par des internautes tiers), et que les effets inter-expansifs de ces relations entre prescriptions agrandissent l'échelle du rapport de force interhumain dans le cas JVC.

Troisièmement, en publiant des messages injurieux au moyen des deux compétences étudiées (celles obtenir de la concrétisation ordonnée qu'elle respecte fidèlement et qu'elle accroisse constamment leurs demandes et volontés), les récalcitrants apportent la preuve que *chacun* d'entre eux est *également* titulaire de ces compétences. La compétence ainsi *décentralisée* et *horizontale* de faire concrétiser une prescription en ligne préservatrice et amplificatrice de contenus injurieux garantit aux récalcitrants l'**impossibilité pour quiconque** (un régulateur, un gestionnaire de logiciel, les autres internautes...) **de retirer cette compétence à son titulaire humain ou de la hiérarchiser** (selon son titulaire, les contenus produits, son exercice manuel par l'internaute ou automatique par un logiciel...). Dans ces conditions, il n'appartient qu'au récalcitrant de concrétiser la prescription dont il est l'auteur pour attacher à sa volonté et à sa demande les effets préservateurs et amplificateurs d'une diffusion en ligne. Bien sûr, la titularité de ces compétences au bénéfice des récalcitrants n'empêche pas le gestionnaire du logiciel de contre-attaquer en produisant à son tour des prescriptions en ligne. Il peut par exemple créer une fonctionnalité de signalement des contenus injurieux à disposition des internautes, et une autre fonctionnalité de suppression des contenus signalés à disposition des modérateurs. Ces fonctionnalités, préservées dans leur intégrité par le serveur qui les héberge, amplifient leur concrétisation à chaque accès ordonné par l'internaute auteur du signalement ou le modérateur censeur. Comme les prescriptions manuellement produites par les récalcitrants, ces deux prescriptions logicielles produites par le gestionnaire doivent leur préservation à un serveur aliéné (vis-à-vis de l'instruction logicielle hébergée et des requêtes d'accès adressées) et leur amplification à leur disponibilité sur le réseau (qui en permet ainsi la concrétisation par toute machine connectée au même réseau). De même, tout comme le récalcitrant ne peut prescrire qu'en vertu la possibilité technique également ouverte à tout être humain de produire des données manuelles, le gestionnaire ne peut prescrire qu'en vertu de la possibilité technique également ouverte à tout être humain de produire une règle logicielle. En somme, que la production de données soit manuelle ou automatisée, la concrétisation d'une prescription en ligne dépend des mêmes compétences de produire de manière ouverte/aliénante/inaltérée des prescriptions disponibles/ubiquitaires/inter-expansives grâce à un pouvoir technique décentralisé/horizontal. **Quelle que soit la prescription en ligne** (manuelle/logicielle), **qui que soit son auteur, elle résulte toujours de l'exercice des mêmes compétences numériques par l'être humain.**

Que notre analyse du pouvoir de l'internaute ait pris pour point de départ le fonctionnement interne de la machine connectée (comme on l'a fait *supra* en illustrant la modélisation complexe des PN avec le cas JVC) ou bien le rapport de force interhumain qui lui est externe (comme on vient de le faire en illustrant avec ce même cas l'utilisation humaine faite de la machine connectée), on parvient systématiquement à la conclusion d'un pouvoir prescriptif effectivement exercé par l'internaute et on relève chaque fois les mêmes caractéristiques prescriptives. Par cette double confirmation, l'explication prescriptive ici proposée nous semble éclaircir le « mystère » du pouvoir endogène de l'internaute dans le cas JVC : **si l'internaute peut gagner un rapport de force l'opposant au gestionnaire d'un logiciel, c'est parce que cet internaute tient du fonctionnement interne à la machine connectée un pouvoir prescriptif numérique en ligne**. De ce fait, il peut imposer et amplifier des prescriptions susceptibles de contredire voire de concurrencer les prescriptions produites par le gestionnaire (en rendant inefficace un algorithme de modération dans le cas d'espèce). En réponse, la riposte numérique du gestionnaire est également exprimée par des prescriptions binaires imposées et amplifiables (création de nouvelles fonctionnalités, modification des précédentes, utilisation de celles actuelles comme la suppression des contenus...). Le rapport de force interhumain qui voit l'internaute résister à l'algorithme modérateur du gestionnaire, puis celui qui voit ensuite le gestionnaire répliquer à l'internaute, sont tous deux le fruit des actions numériques prescriptives produites par ces internautes et gestionnaire.

La prescription en ligne se fait l'arme binaire avec laquelle se disputent les rapports de force interhumains via un réseau numérique. Aussi les internautes n'hésitent-ils pas à se servir de cette arme lorsqu'ils souhaitent s'imposer dans un tel rapport de force en ligne. On l'observe par exemple dans un « deuxième cas JVC » : en 2019, après que l'entreprise Oasis ait organisé le 26 juin un concours sur Twitter récompensant la ville la plus citée avec le hashtag #OasisStreetCan en distribuant dans cette ville des canettes de soda gratuites à son nom, la communauté du forum JVC s'est coordonnée pour citer massivement la commune d'Issou⁴¹⁶. En agissant ainsi, cette communauté prescrit au serveur de Twitter la publication de chacun des tweets citant la commune d'Issou associée au #OasisStreetCan. Ces prescriptions se heurtent toutefois à celles produites par une autre communauté, idéologiquement rivale à la communauté JVC, péjorativement baptisée ou parfois autoproclamée *Social justice warrior*, couramment abrégée SJW. Radicalement voire agressivement défenseuse de l'égalité (par le recours à des insultes, menaces, demandes abondantes de suppression de contenus qu'elle juge sexistes, homophobes, handiphobes, racistes...) cette communauté rivale a mené fin juin 2019 une campagne de tweets dénonçant l'instrumentalisation du concours par la communauté JVC et la complicité d'Oasis avec un forum « haineux » si la multinationale avait le malheur de déclarer Issou vainqueur du concours. Cette campagne numérique prescrite par les SJW aux serveurs de Twitter aboutit au verdict annoncé dans un tweet publié par Oasis le 2 juillet 2019 : « *suite à la mobilisation de la communauté du forum JVC 18-25, la ville d'Issou a gagné haut la main ce concours grâce à des tweets qui étaient jusqu'à présent bienveillants et respectueux. Malheureusement, depuis l'annonce de la ville gagnante, les propos inacceptables de certains membres associés au forum JVC nous obligent à exclure la ville d'Issou du concours car ce qu'elle représente (malgré elle) et les tweets associés sont totalement contraires aux valeurs de la marque Oasis* ». La réaction de la communauté JVC ne se fait pas attendre : le 3 juillet, après s'être une fois de plus

416Le choix de la ville par la communauté JVC se réfère au même *Risitas* – un courte vidéo (généralement sous format .gif) extraite d'une émission de télévision espagnole, dont le rire d'un des invités (Juan Joya Borja) laisse entendre « Issou » lorsqu'il prononce « Jesús ». Maints fois détourné en ligne, ce même est devenu un emblème de la communauté JVC.

coordonnée depuis son forum, elle parvient à faire se hisser en première place des hashtags « Tendances Twitter France » (i.e. des # les plus visibles publiquement tels que classés par l'algorithme de Twitter) le #BoycottOasis, accusant profusément la marque Oasis de « *truquer* » ses concours sous la pression des SJW. Dans ce deuxième cas JVC, les coordinations communautaires, les dénonciations par les SJW, le verdict d'Oasis et les boycotts accusateurs du JVC retranscrivent en ligne des prescriptions ordonnées par ces acteurs aux machines impliquées. Que les rapports de force opposent des internautes et un gestionnaire de logiciel (1^{er} cas JVC) ou exclusivement des producteurs manuels de données (2^e cas JVC), **c'est à coups de prescriptions que des rapports de force interhumains se construisent, s'aggravent et se résolvent par prescriptions numériques interposées.**

Ce constat vaut également lorsque les rapports de force interhumains en ligne quittent le contexte communicationnel. Il en va ainsi d'une cyberattaque, qui n'a pas nécessairement le format d'une communication sociale (tels un message ou une interface graphique) mais plus souvent celui d'un code source seulement. Le logiciel malveillant (*malware*) une fois installé sur la machine cyberattaquée, c'est ce code source qui engendre une action numérique en prescrivant, par instruction logicielle, sa concrétisation à la machine l'hébergeant. Si une cyberattaque peut déployer son action et ainsi engendrer un rapport de force interhumain, c'est donc parce que cette cyberattaque *prescrit* par instruction logicielle sa concrétisation à la machine qui en est victime. Malgré l'absence de contexte socio-communicationnel, un rapport de force interhumain en ligne par lequel le cyberattaquant s'impose au cyberattaqué jaillit à nouveau de prescriptions binaires produites sur un réseau numérique et opérant selon les modalités décrites (préservation de l'intégrité de la prescription malveillante, amplification de sa concrétisation par le nombre de machines connectées impliquées, possibilité égale et individuelle de produire une prescription malveillante). Ou encore, lorsqu'un internaute télécharge un *AdBlocker* dont il active les fonctionnalités pour dissimuler les publicités présentes sur une page web, cet internaute prescrit l'exécution de cette fonctionnalité qu'il impose aux annonceurs voire au gestionnaire du logiciel sans pour autant produire de communication sociale. Par conséquent, **la « communication » n'est qu'un format et non une cause du rapport de force interhumain né de prescriptions en ligne.**

Réalisée à l'échelle des communications, une étude des rapports de force interhumains en ligne ne couvre donc que partiellement l'étendue du pouvoir prescriptif en ligne. Consacré aux communications accessibles à la compréhension sociale humaine, un tel champ d'étude exclut les rapports de force interhumains en ligne non-communicationnels, et par là les pouvoirs exercés dans le cadre de ces rapports de force tant par l'auteur d'un logiciel (par ex. d'une cyberattaque) que par l'internaute (par ex. le téléchargement et l'activation d'un *AdBlocker*). Si **l'approche exogène communicationnelle** est pertinente à son échelle pour connaître les effets et pouvoirs sociaux associés aux communications humaines en ligne⁴¹⁷, elle **ne nous semble pas permettre**

417 Dans une telle perspective exogène, la « prescription » a une signification bien différente de la nôtre puisqu'elle est identifiée à partir de son insertion dans un contexte non plus numérique-binaire mais social-humain. Dès lors, la prescription n'est pas recherchée dans la compréhension machinale mais dans la compréhension humaine (une loi juridique, l'ordre d'un employeur, un conditionnement cognitif ou opérationnel de la demande par l'offre...). Bien plus que d'un acte momentané d'exécution, la validation d'une telle prescription « communicationnelle » résulte alors de sa réception sociale qui en assure l'évolution constante. Au lieu d'être une source certaine d'exécution telle qu'on l'a établi pour la prescription endogène (i.e. socialement décontextualisée), la prescription communicationnelle est une « *source potentielle d'influences* » qui ne joueront qu'avec la

de tirer de conclusions sur le pouvoir (qu'elle ne couvre que partiellement) **dont disposent les acteurs en ligne du fait de leur production de données binaires sur un réseau numérique.**

On ne peut donc trouver de cause communicationnelle à chacun des rapports de force interhumains en ligne examinés (opposant des internautes et un gestionnaire de logiciel, des internautes entre eux, un cyberattaquant et un cyberattaqué, des internautes et des annonceurs...) mais on peut génériquement leur trouver une cause endogène rapportable aux prescriptions numériques. On sait déjà que toute donnée binaire en ligne est comprise par la machine numérique comme une prescription car chacune porte une règle logicielle exécutable et applicable par cette machine et dont l'accomplissement procède d'un ordre (instruction logicielle ou instruction machine issue du producteur de données). On vient de constater en pratique que, par sa production de données, l'être humain exerce des compétences comprises comme prescriptives pour la machine (compétences de produire de manière ouverte/aliénante/inaltérée des prescriptions disponibles/ubiquitaires/inter-expansives grâce à un pouvoir technique décentralisé/horizontal), et que l'utilisateur de cette machine génère des rapports de force interhumains en exerçant ainsi ses compétences. On en déduit que les rapports de force interhumains qui naissent d'une production de données binaires en ligne résultent nécessairement de compétences prescriptives attribuées à l'être humain par des lois numériques régissant la compréhension de la seule machine connectée (lois de neutralité et d'interopérabilité exécutives, de solidarité application, d'interconnexions binaire, protocolaire et opérationnelle). On peut dès lors **apporter confirmation à la seconde hypothèse** faite plus haut selon laquelle, comme l'activité atomique interne à l'objet physique (par ex. radioactivité) modifie les rapports de force interhumains externes nés de l'utilisation de cet objet (par ex. armes nucléaires), **l'activité prescriptive connue par la machine** (p. ex. interactions de prescriptions en ligne et échelle de diffusion d'une donnée issue de l'exécution d'une prescription en ligne) **influence les rapports de force interhumains externes nés de l'utilisation de cette machine** (par ex., amplification des volontés, demandes et actions humaines). Pour le dire autrement, **c'est en qualité de « prescriptions numériques » que les données binaires humainement produites en ligne peuvent entraîner des rapports de force interhumains.**

Section 3. Les leçons des échecs de l'explication Code Is Law

Tandis que la théorie *Code is Law* échoue à expliquer de nombreux phénomènes observés en ligne, la théorie qu'on propose des prescriptions numériques permet d'expliquer : l'existence

reconnaissance de la prescription par ses destinataires (DOMENGET Jean-Claude, « Prescription, recommandation, exploration : une approche temporaliste des usages des médias socionumériques » [en ligne], *Études de communication*, n° 49, 2017). Au lieu d'être définitivement arrêtée par son producteur comme on l'a établi pour la prescription endogène, la prescription communicationnelle est coconstruite avec les destinataires susceptibles de rejeter la prescription émise, qui ne cessera d'évoluer en s'insérant socialement (« prescription par les pairs », *ibid.*). Inspirée des travaux d'Armand Hatchuel (qui identifie des « marchés prescripteurs »), cette théorisation conçoit la prescription comme instable en société, changeante par le jeu des acteurs sociaux – là où notre approche endogène nous fait au contraire tenir une prescription pour figée dans son contenu (bien qu'évolutive dans son effectivité) tel que ce contenu est unilatéralement établi par le prescripteur. Par ex., le chercheur en sciences de l'information et de la communication Pierre Delcambre, renouvelant les théories d'A. Hatchuel, identifie la prescription moins à l'échelle d'une activité sur le marché – comme un métier – qu'à l'échelle d'une « *opération sociale* » induisant le travail contributif d'acteurs sociaux » (DELCAMBRE Pierre, « Prescrire comme opération sociale », *Territoires contemporains*, 2019 [en ligne sur tristan.u-bourgogne.fr])

des diverses sources de contrainte directe sur la compréhension machinale qui dépassent la seule source des programmeurs (Paragraphe 1) ; et l'interdépendance de ces sources de contraintes, due au fait que le cyberspace est un bien commun (Paragraphe 2).

Paragraphe 1. L'effondrement de l'explication *Code is Law*

Après avoir constaté que la contrainte machinale est le résultat du code binaire plutôt que du code source (A), on en déduira six catégories de prescripteurs numériques parmi les êtres humains (B).

A) Le code binaire, cause de la contrainte machinale

Pour rappel, les partisans de l'explication CodIL (L. Lessig en droit constitutionnel, S. Turkle en psychologie, D. Cardon et P. Flichy en sociologie, P. Mathias et A. Rouvroy en philosophie...) tiennent le code source pour la cause endogène du pouvoir contraignant exercé en ligne. Les maîtres de ce code source (développeur, administrateur d'un logiciel, hacker...), en décidant de la possibilité ou de l'impossibilité des actions logicielles, seraient faiseurs des capacités numériques : quelle que soit l'action en ligne⁴¹⁸, elle découlerait toujours d'une règle élaborée par un maître du code source. L'explication CodIL réserve alors aux maîtres du code source le pouvoir de contraindre les autres acteurs internes au réseau par la détermination de leurs capacités d'action en ligne.

Plus un code source accessible en ligne compte d'utilisateurs (par ex., le logiciel d'une plateforme à succès comme certains « géants numériques » – Amazon, Reddit, Pornhub, WhatsApp...), plus le maître de ce code étend à un grand nombre d'actions en ligne son pouvoir d'en établir les modalités (étapes d'achat, moyens de paiement ou encore biens autorisés à la vente tels que déterminés par une place de marché en ligne, suites de caractères publiables sur un forum selon les décisions de son administrateur, formats conditionnant la mise en ligne d'une vidéo et fixés par le propriétaire du logiciel, droit conféré à l'utilisateur par le développeur d'ouvrir un message sans que l'interlocuteur en soit averti...), d'en limiter le périmètre (périmètre géographique défini pour qu'un utilisateur puisse acheter un bien en ligne ou se le voir livrer, présence en ligne d'un message dont l'accès requière une action volontaire d'y accéder par l'utilisateur d'un forum ou est au contraire imposé à l'utilisateur d'un réseau social par notification ou insertion dans son « fil d'actualités », nombre ou poids maximum de vidéos publiables par jour avec et sans abonnement au service, catégories d'utilisateurs capables de recevoir le message d'un autre utilisateur tels que les « contacts »...), d'en empêcher la survenance (censure algorithmique préventive empêchant la publication, sur un forum, d'une image violant des droits d'auteurs ou, sur une place de marché, d'une proposition de vente dont la présentation du produit correspond à des substances stupéfiantes, censure répressive interdisant à un utilisateur de produire des actions sous son compte habituel, impossibilité de lancer la lecture d'une vidéo pornographique sans la présentation d'une pièce attestant la majorité civile de l'utilisateur ou impossibilité de « disliker » un contenu en ligne...), de les soumettre aux actions génériques du maître du code source (valorisation par algorithme suggestif de produits en vente, classification des messages selon l'interface d'un forum ou d'un réseau social, gratuité des contenus pornographiques pour tous les utilisateurs le jour de la Saint-Valentin...) etc. Les moyens de l'action en ligne étant suspendus aux choix faits par le maître du code source, seule la maîtrise

418LESSIG L., *Code: Version 2.0*, préc., 2006, p. 283 : « *il est (...) peu probable qu'une personne entrant dans [l'espace virtuel d'un jeu vidéo] ne remarque pas qu'une dimension importante de cette construction est la construction par le code. Votre capacité à voler [fly] est un choix des codeurs. L'endroit jusqu'auquel vous pouvez voler est un choix des codeurs. L'affichage d'un message d'avertissement lorsque vous heurtez quelqu'un est un choix des codeurs. Votre capacité à désactiver les conversations instantanées des personnes que vous ne voulez pas entendre est un choix des codeurs. Personne ne se méprend sur le fait que des choix sont faits ici.* »

d'un tel code offrirait un contrôle des capacités d'agir numériquement⁴¹⁹. Pivots de la régulation CodIL⁴²⁰, les maîtres des programmes informatiques sont alors l'unique catégorie d'acteurs à laquelle est reconnu le pouvoir de prescrire des règles contraignantes dans l'activité interne au réseau (ou « cyberspace » d'après le vocabulaire de L. Lessig).

L'explication CodIL est toutefois mise en échec par le premier cas JVC qu'on a rapporté. En l'espèce, les utilisateurs n'ont aucun pouvoir de contrôle sur le code source du forum JVC. Pourtant, ils contraignent non seulement leurs propres terminaux mais surtout les serveurs de JVC à exécuter leurs requêtes, pour persister à publier des contenus haineux malgré la censure opérée via le code source. En ordonnant ainsi l'exécution de prescriptions numériques par les serveurs de JVC, les internautes gagnent ce rapport de force contre l'administrateur du forum JVC. Ce cas illustre l'absence de contrôle du programmeur du forum JVC sur les contraintes qu'imposent les internautes aux machines dont dépend ce forum (notamment les serveurs).

Comment expliquer ce manque de contrôle du programmeur sur les actions des internautes ? L'internaute pourrait-il créer ses propres règles ? Techniquement, l'internaute ne peut pas créer ses propres règles : seul le programmeur peut créer, au moyen du code source, des PN abstraites, des règles exécutables et applicables. Prenons l'exemple de l'utilisateur Bob qui souhaite publier en ligne, sous un article du journal Le Monde, le commentaire suivant : « *les arabes remplacent les français* ». Supposons qu'il souhaite effectuer cette action depuis l'application mobile Le Monde téléchargée sur son smartphone. En demandant la publication de son message, Bob utilise donc les instructions logicielles de l'application Le Monde stockées sur son smartphone. On a vu que toutes les instructions logicielles reposent fondamentalement sur le langage machine. Les fonctions proposées à l'utilisateur par l'application mobile Le Monde dépendent donc d'instructions logicielles qui puisent uniquement dans les ressources du langage machine : la fonction « publier un commentaire » proposée par Le Monde résulte d'instructions logicielles qui combinent diverses instructions machines et/ou préalables ; la fonction « insérer des caractères » proposée par Le Monde s'appuie sur la table des caractères stockée nativement dans le smartphone de Bob. Bob ne peut donc formuler sa requête qu'en se fondant sur les instructions logicielles du Monde, elles-mêmes fondées sur le langage machine. Seul le programmeur peut créer des PN abstraites (règles exécutables et applicables par la machine), et l'utilisateur ne peut produire des requêtes qu'en manipulant les PN abstraites stockées dans sa machine.

L'explication CodIL a donc pour mérite d'avoir souligné ce fait technique selon lequel les capacités d'action des utilisateurs sont entièrement dépendantes des programmeurs. Dès lors,

419LESSIG L., « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 [en ligne sur le site d'Harvard Magazine] : « *La question n'est donc pas de savoir qui décidera de la manière dont le cyberspace est régulé : ce seront les codeurs. La seule question est de savoir si nous aurons collectivement un rôle dans leur choix – et donc dans la manière dont ces valeurs sont garanties – ou si nous laisserons aux codeurs le soin de choisir nos valeurs à notre place.* »

420LESSIG L., *Code: Version 2.0*, p. 121, préc. : « *je crois que le cyberspace crée une nouvelle menace pour la liberté, pas nouvelle dans le sens où aucun théoricien ne l'avait conçue auparavant, mais nouvelle dans le sens où elle devient urgente. Nous commençons à comprendre qu'il existe un nouveau régulateur puissant dans le cyberspace. Ce régulateur pourrait être une menace importante pour un large éventail de libertés, et nous ne connaissons pas encore la meilleure façon de le contrôler. Ce régulateur est ce que j'appelle le "Code" – les instructions intégrées dans le logiciel ou le matériel qui font du cyberspace ce qu'il est. Ce code est l'"environnement bâti" de la vie sociale dans le cyberspace. Il est son "architecture".* »

l'utilisateur n'a pas la capacité de créer des règles exécutables et applicables, et **le manque de contrôle du programmeur sur les actions de l'utilisateur** ne peut s'expliquer par une telle capacité inexistante. Il **s'explique par la distinction entre les capacités d'action de l'utilisateur et ses actions réelles, entre les PN abstraites et les PN concrètes**. Par exemple, au-delà des technologies, les capacités d'action naturelles d'un être humain lui offrent d'exploiter ces capacités ou de ne pas les exploiter, et même de combiner ces capacités pour obtenir un résultat nouveau (telle que l'invention de la roue par l'être humain). Le fait que les lois de la physique et de la biologie aient donné ces capacités à l'être humain ne signifie pas que ces lois contrôlent les actions réelles des êtres humains et les résultats nouveaux qu'ils produisent. Ce raisonnement est aussi valable pour les technologies numériques : le programmeur définit certes les capacités d'action des utilisateurs, mais les utilisateurs peuvent ne pas exercer ces capacités, ou peuvent les combiner pour obtenir un résultat informatique nouveau. L'utilisateur peut ainsi, à l'appui des capacités d'action fournies par le programmeur, produire un résultat informatique inattendu et incontrôlable par le programmeur.

En pratique, tout utilisateur peut à tout moment produire un résultat informatique inattendu en combinant des données de caractère voire des données d'instruction. Concernant les données de caractère, cette hypothèse renvoie au premier cas JVC, ou encore à l'exemple du « drapeau LGBT barré ». Sur ce dernier exemple, depuis 2016, les utilisateurs ont la capacité de combiner des emojis. En 2019, de nombreux utilisateurs ont exploité cette capacité d'action pour combiner l'emoji du drapeau LGBT avec l'emoji du cercle barré, de façon que les deux emojis se superposent pour laisser apparaître un drapeau LGBT barré. Ce symbole a été notamment employé en guise de message homophobe et, à ce titre, est potentiellement illicite (par exemple s'il est envoyé en masse ou de manière répétée à un utilisateur homosexuel). Bien qu'Unicode — le consortium décidant des nouveaux emojis — n'ait jamais validé cette combinaison spécifique d'emojis, le drapeau LGBT barré a été très largement diffusé⁴²¹. On verra que les caractères sont souvent combinés par les utilisateurs afin de contourner la censure. Outre les caractères, les utilisateurs peuvent aussi combiner les données d'instruction, par exemple dans le cadre d'une attaque par déni de service (DDoS). P. ex., une communauté d'utilisateurs peut s'équiper d'un logiciel qui produit automatiquement des requêtes, et détourner l'usage de ce logiciel en adressant automatiquement et massivement des requêtes à un même serveur afin d'en saturer les capacités de stockage ou d'exécution. Le(s) sites hébergés par ce serveur seront alors inaccessibles.

Le programmeur n'a pas de contrôle sur la contrainte concrète qu'impose l'internaute à la machine, il n'a pas de contrôle sur les données que combine l'utilisateur dans un cas concret, et n'a donc pas de contrôle sur le résultat informatique de l'action de l'internaute. Le programmeur n'a de contrôle que sur les PN abstraites qu'il crée, et non sur les PN concrètes produites par les utilisateurs du programme dans le cadre de leurs requêtes.

Le pouvoir du programmeur sur l'utilisateur doit alors être nettement relativisé par rapport à ce qu'enseigne la théorie CodIL. D'abord, le programmeur n'a pas de contrôle sur les actions réelles de l'internaute⁴²². Cela nous permet d'en conclure que **la maîtrise du code de programmation n'est pas le seul foyer contraignant l'activité interne au réseau**, puisque les

⁴²¹ SIGNORET Perrine, « Non, il n'existe pas d'"emoji anti-LGBT" », *Numerama*, 22 fev. 2019

⁴²² Les capacités d'action de l'utilisateur se diversifient non selon le nombre de capacités fixées par un code de programmation mais selon le nombre de combinaisons possibles entre les règles conçues par les programmeurs et accessibles à l'utilisateur

productions de données par les internautes sont également contraignantes pour cette même activité comprise des machines connectées. Ensuite, les données produites par un internaute peuvent gagner sur internet une échelle de diffusion supérieure à celle d'un logiciel conçu par un programmeur et méconnu du public, de sorte que la contrainte exercée par un utilisateur peut impliquer un plus grand nombre de machines dans le monde que la contrainte exercée par un programmeur. Enfin, et surtout, le programmeur et l'utilisateur tiennent leur pouvoir de contrainte (endogène) de la même source : le code binaire.

En effet, que la prescription soit produite par langage machine (PN abstraite), langage logiciel (PN abstraite) ou dans le cadre d'une requête (PN concrète), elle contraint la compréhension et l'exécution de la machine en vertu de la neutralité avec laquelle cette machine concrétise une action formulée binairesment. On a démontré en premier lieu que *la neutralité de la machine implique son aliénation à l'ordre du prescripteur*. Ainsi aliénée par l'action impérative du prescripteur, la machine y est contrainte. Le pouvoir de contraindre une machine numérique s'exerce donc grâce à l'aliénation de cette machine à l'action du prescripteur. On a démontré en second lieu que *cette aliénation et ce pouvoir de contrainte ne valent que pour des actions formulées en code binaire*. Les actions dépourvues d'un tel format binaire sont ainsi privées d'effet numérique contraignant car, incomprises par la machine, cette dernière ne saurait y être aliénée. Par conséquent, toute action produite doit l'être en code binaire pour contraindre la machine et obtenir concrétisation. En somme, quel que soit **le prescripteur en ligne** concerné, **il tire son pouvoir contraignant (endogène) de rien d'autre que l'aliénation de la machine numérique au code binaire**. Pour le dire en termes moins théoriques, **toute production de données binaires et seule une production de données binaires peut contraindre la machine à comprendre et à exécuter des données**.

B) Les différents prescripteurs numériques

L'explication CodIL échoue à couvrir plusieurs phénomènes numériques majeurs : si comme le prétend l'explication CodIL le pouvoir de contrainte est imputable à la maîtrise du code de programmation plutôt qu'à celle du code binaire, comment expliquer que le maître du code de programmation soit incapable de contraindre la moindre machine numérique tant que son code n'est pas formulé binairesment – et inversement, comment expliquer que l'utilisateur non-maître d'un code de programmation soit capable générer des données contraignantes pour la machine sous leur format binaire ? Si l'utilisateur est dépourvu d'un pouvoir de contrainte de même nature que celui du programmeur, comment expliquer que la capacité de l'un et de l'autre à contraindre ainsi la machine résulte de la même cause technique (aliénation de la machine au code binaire) ? Si l'utilisateur dépend exclusivement du programmeur, comment expliquer techniquement l'absence de contrôle du programmeur sur les actions réelles et les résultats informatiques de l'utilisateur ? Enfin, si l'action du programmeur est systématiquement plus contraignante que celle de l'internaute, comment expliquer que certaines actions de l'internaute contraignent davantage de machines connectées que ne le font certaines actions du programmeur ?

A contrario, l'explication prescriptive qu'on soumet dans cette thèse avance une réponse pour chacun de ces phénomènes. Aliénée par le code binaire, la machine est contrainte par toute action numérique produite (abstraitemment par le stockage d'un logiciel ou concrètement dans le cadre d'une requête). Toute production de données binaires est alors constitutive d'une prescription numérique (i.e. d'une règle exécutable et applicable dont l'accomplissement procède d'un ordre binaire).

Chaque producteur de données binaires étant ainsi producteur de prescriptions numériques, l'utilisateur possède à ce titre un pouvoir prescriptif numérique concret qui lui est propre, affranchi de la maîtrise du programmeur (cantonnée à son seul code de programmation) et par lequel l'utilisateur maîtrise lui-même une combinaison contraignante de règles programmées. L'utilisateur et le programmeur détiennent dès lors un pouvoir numériquement contraignant de même *nature* prescriptive, c'est-à-dire *né* de la même cause : le code binaire. De même nature, les actions produites par chacun détiennent les mêmes attributs que ceux de toute prescription numérique - une portée ubiquitaire due à leur stockage sous format binaire quelle que soit la machine concernée, et une portée ordonnatrice due à l'exécutabilité de toute donnée binaire par n'importe quelle machine numérique. Par leur portée ubiquitaire, les données produites par l'internaute comme celles produites par le programmeur sont toujours disponibles d'accès sur le réseau ; par leur portée ordonnatrice, les données produites peuvent contraindre n'importe quelle machine à exécuter ces données, offrant ainsi à n'importe quelles données la possibilité d'acquérir une échelle de diffusion aussi étendue que le nombre de machines connectées à internet. Cette théorie prescriptive propose par-là une explication technique du phénomène qui voit l'action de l'internaute contraindre les machines connectées parfois plus vastement que l'action du programmeur.

Au lieu d'une activité interne au réseau contrainte par les seuls programmeurs maîtres de sa régulation (explication CodIL), **on décèle une activité interne au réseau contrainte par tout producteur de données numériques binaires et régie par les prescriptions numériques issues de cette production** (explication prescriptive). Contrairement à la thèse soutenue par l'explication CodIL, **le pouvoir de produire des actions contraignantes internes au réseau ne résulte donc pas de l'aliénation de la machine au code de programmation** (maîtrisable par les seuls programmeurs), **mais de l'aliénation de la machine au code binaire** (maîtrisable par tout acteur produisant une donnée binaire). Les perspectives de l'analyse endogène des rapports de force interhumains en ligne sont alors profondément renouvelées par un effondrement de l'explication CodIL.

Premièrement, le fait de considérer le code binaire comme la source de la contrainte endogène nous permet d'identifier les différents prescripteurs numériques en ligne. On sait d'abord que tout prescripteur en ligne est un producteur de données binaires portant une instruction, et que tout producteur de données binaires portant une instruction est un prescripteur en ligne. On distingue les prescripteurs numériques à l'aide de trois critères : le support de la production de données binaires ; les techniques de production de données binaires ; et le type de PN produites (abstraites ou concrètes). Sur le premier critère, on observe quatre types de supports connectés à internet et capables de mémoriser des données binaires produites : (i) les terminaux ; (ii) les serveurs ; (iii) les routeurs ; (iv) et les périphériques accessoires. Les terminaux ont pour fonction de permettre à l'utilisateur final de produire des données, et incluent diverses machines : l'ordinateur, le smartphone, la tablette, la console de jeux, la télévision connectée...

Les serveurs ont pour fonction de fournir à l'utilisateur final un service hébergé sur internet : les serveurs d'applications hébergent les applications (*i.e.* les services auxquels accède définitivement l'utilisateur, tel un site web ou un jeu vidéo) ; les serveurs DNS hébergent les noms de domaine ; les serveurs de bases de données hébergent les bases de données des applications etc. Les routeurs ont pour fonction d'acheminer les données entre le terminal de l'utilisateur et le serveur. Enfin, on appelle « périphérique accessoire » tout périphérique qui sert d'accessoire à un terminal, un

serveur ou un routeur. Cette catégorie inclut notamment les disques durs externes, les clés USB, les disques de stockage optique (CD, DVD...), les cartes mémoire ou encore les objets connectés. Tandis que les quatre premiers périphériques cités sont généralement des accessoires d'un terminal, les objets connectés sont des accessoires des serveurs : la connexion d'un objet connecté au réseau internet dépend de sa connexion à un serveur lui-même connecté à ce réseau. Le service proposé par ce serveur consiste à fournir au terminal de l'utilisateur des fonctionnalités d'accès voire de contrôle de l'objet connecté (assistant personnel intelligent, lampe, montre, bracelet, voiture, drone, radiateur, jouet...). Pour utiliser un objet connecté, l'utilisateur doit donc accéder depuis son terminal (p. ex. son smartphone) au serveur dont dépend cet objet. Ces quatre supports de production de données nous permettent déjà d'en déduire cinq catégories d'êtres humains capables de produire des prescriptions numériques à partir de ces supports : **le fabricant** (du terminal, du routeur, du serveur ou du périphérique accessoire) ; **l'utilisateur** du terminal ; **l'opérateur** gestionnaire des routeurs, pour transmettre les données entre l'utilisateur et le serveur ; **l'administrateur d'une application** (Facebook, Google, Snapchat...), qui fait héberger son logiciel sur un serveur pour le mettre à disposition de l'utilisateur ; et le **gestionnaire du serveur**, qui met ses serveurs à disposition de l'administrateur d'une application pour héberger cette dernière et les fichiers nécessaires à son fonctionnement (bases de données, logiciels de gestion de l'application par l'administrateur...).

Sur le deuxième critère des techniques de production de données binaires, les deux techniques basiques sont la production manuelle ou automatisée de données. On appelle « production manuelle » de données le fait, pour le producteur, de devoir définir à nouveau sa production chaque fois qu'il souhaite la répéter. Inversement, on appelle « production automatisée » de données le fait, pour le producteur, de pouvoir répéter sa production de données sans devoir la redéfinir à chacune de ses répétitions. Habituellement, l'utilisateur produit manuellement des données, mais il peut en produire automatiquement à l'aide d'un logiciel qui automatisera son action. L'utilisateur n'est pas un profil identifiable à partir de la technique de production de données, mais à partir du fait qu'il utilise un programme. Quant au programmeur, s'il doit certes produire des données manuellement pour créer son logiciel, le logiciel qu'il programme lui permet d'automatiser la production de données. Ce pouvoir du programmeur résulte précisément de sa capacité à produire des PN abstraites : la règle abstraite issue de l'action créatrice du programmeur étant générique, il n'est nul besoin pour ce programmeur d'agir à nouveau en recréant cette règle chaque fois qu'est sollicitée sa concrétisation. Abstraction valable, l'action contraignante prévue par cette règle peut être réitérée sans qu'il soit nécessaire de réitérer la création concrète de cette règle. On distingue trois types de programmeurs en fonction du type de logiciels qu'ils créent : le programmeur peut concevoir un programme en langage machine (table des caractères, table des exceptions et interruptions, *General Descriptor Table* qui définit la mémoire virtuelle de la machine...), auquel cas ce programmeur travaille le plus souvent aux côtés du fabricant ; il peut concevoir un système d'exploitation (Windows, Android, macOS...), qui permet aux applications de fonctionner sur la machine ; et il peut concevoir une application locale (service logiciel stocké sur un terminal, comme Word, Excel, Acrobat, Photoshop...) ou une application en ligne (service logiciel stocké sur un serveur, comme un site web, un jeu vidéo, un réseau social...).

Enfin, sur le troisième critère, parmi ceux identifiés, les acteurs qui produisent des PN abstraites sont les suivants : le fabricant ; le programmeur ; et l'administrateur d'applications. Inversement, les acteurs qui produisent des PN concrètes sont les suivants : l'utilisateur ; l'opérateur d'acheminement ; et le gestionnaire de serveurs. En somme, on identifie six

catégories de prescripteurs en ligne recensées ci-dessous. Précisons qu'un prescripteur numérique peut aussi bien être une personne privée (entreprise, citoyen...) qu'une personne publique (agents administratifs agissant en tant qu'utilisateurs, État administrateur de l'application service-public.fr, opérateurs d'acheminement appartenant à l'État comme l'ex-France Telecom, programmeurs travaillant pour le compte de l'administration...).

Les êtres humains producteurs de PN en ligne (prescripteurs numériques en ligne)					
Producteurs de PN abstraites en ligne	Fabricant (programmeur en langage machine)	Programmeur			Administrateur d'applications
		de système d'exploitation	d'applications		
			locales	en ligne	
Producteurs de PN concrètes en ligne	Opérateur d'acheminement	Utilisateur d'un programme			Gestionnaire de serveur

Paragraphe 2. Le cyberspace, à la fois bien commun de fait et réalité prescriptive

Deuxièmement, le fait de considérer le code binaire comme source de la contrainte endogène nous permet d'en tirer une deuxième leçon — outre l'identification des prescripteurs numériques au-delà des seuls programmeurs. En effet, tandis que le code source est appropriable, tel n'est pas le cas du code binaire. Le code binaire est exploitable par toute personne qui utilise une machine numérique. Cela implique que **le pouvoir de contrainte numérique est lui-même inappropriable**. Notre théorie des prescriptions numériques nous mène donc à des conclusions radicalement différentes de celles retenues par l'explication *Code is Law*.

Le caractère inappropriable du code binaire nous fait nous interroger sur la question suivante : le code binaire est-il qualifiable de bien commun ? On reprend ici le concept de « bien commun » des sciences économiques, qui lui reconnaissent deux spécificités d'accès et d'utilisation : le bien commun est à la fois rival (la consommation du bien par un agent en diminue la quantité disponible pour autrui) et non-excluable (aucun agent économique ne peut être exclu de l'accès et de l'utilisation de ce bien sauf exception)⁴²³. Ces deux caractéristiques sont remplies par le code binaire : la production excessive de données binaires a pour effet de saturer les capacités d'exécution du processeur, de sorte qu'une surproduction de données binaires destinées à un même serveur peut rendre ce serveur inaccessible aux autres agents économiques (rivalité du code binaire) ; et aucun agent économique ne peut en principe être exclu de la production de données binaires dès lors qu'il a accès à une machine numérique⁴²⁴ (non excluabilité du code binaire).

⁴²³ Par opposition, le bien privé est un bien rival et excluable, le bien de club est un bien non rival et excluable (cinéma, club sportif, autoroute à péage, brevet...), et le bien public est un bien non rival et non excluable (connaissances scientifiques non brevetées, défense et sécurité, système juridique, éclairage urbain, ponts et autoroutes sans péages...) : WEINSTEIN Olivier, Entrée « Bien public (approche économique) » in CORNU M., ORSI F., ROCHFELD J. (dir.), *Dictionnaire des biens communs*, 2017, préc., p. 89

⁴²⁴ Précisons toutefois que, si le code binaire est un bien commun, une machine numérique est un bien privé

La combinaison de ces deux attributs d'accès et d'utilisation donne naissance à un bien épuisable et pourtant utilisable par une large communauté d'agents économiques. Cela fait courir le risque de la « *tragédie des communs* », c'est-à-dire le risque que le bien disparaisse à cause de sa surexploitation par ses usagers qui abusent des ressources, en consommant ce bien au-delà du seuil nécessaire à sa préservation⁴²⁵. Pour éviter que cette tragédie se produise, l'économiste Elinor Ostrom estime que la solution la plus appropriée et la plus efficace pour la préservation d'un bien commun n'est ni sa privatisation, ni sa nationalisation mais sa gouvernance par la communauté⁴²⁶. En effet, dès lors que les ressources qui alimentent ce bien sont partagées de fait entre ses différents utilisateurs, la privatisation du bien peut entraîner la disparition de ces ressources en les excluant de l'accès au bien, appauvrissant ainsi le bien commun privatisé ; de même, la nationalisation du bien commun rattache sa gestion à la personne publique, et la détache de la communauté qui alimente ce bien en lui apportant ses propres ressources. Dès lors, ces deux solutions « coupent » le bien de ses ressources, et la gouvernance du bien par la communauté de ses utilisateurs apparaît comme la solution la plus adaptée.

Au titre de cette gouvernance collective, E. Ostrom distingue deux types de biens communs : ceux qui concernent une communauté de petite taille (pâturage, pêche, champ irrigué...), qui peuvent être gouvernés en confiant la propriété du bien à tous les membres de la communauté dans le cadre d'une seule et unique structure de gouvernance ; et ceux qui concernent une communauté de grande taille (air, climat, océan...), qui requièrent pour leur gouvernance une « *organisation multi-niveaux d'entreprises inter-reliées avec de petites entités au niveau de base* »⁴²⁷. En somme, on peut définir le **bien commun** comme **tout bien rival et non-excluable, qui obtient ses ressources grâce à la communauté de ses utilisateurs dont les membres se partagent ainsi de fait lesdites ressources, et qui appelle donc une gouvernance communautaire pour préserver l'intégrité et les ressources apportées à ce bien**. On a vu que le code binaire est rival et non-excluable. Par ailleurs, le code binaire ne survit que grâce à la communauté de ses utilisateurs : si aucune personne n'utilise de machine numérique, le code binaire existera certes toujours dans la machine mais il ne sera jamais exécuté, et n'acquerra donc aucune réalité dans un cas concret. De même, le code binaire est exposé à la tragédie des communs si, comme on l'a vu, les utilisateurs abusent de la production de données binaires, au point de rendre inexécutables et inapplicables les autres requêtes binaires. Le code binaire apparaît donc comme un bien commun, dont les ressources partagées reposent sur les requêtes binaires et les capacités d'exécution du code binaire par le processeur.

Quant à savoir si le code binaire est un « commun », cela demande de différencier le *bien commun* du *commun*. Le bien commun l'est toujours de fait, il réunit par lui-même les caractéristiques rapportées. Il ne possède donc pas une gouvernance qui garantit sa préservation ou son intégrité, mais nécessite une telle gouvernance pour s'épargner la tragédie décrite par G. Hardin. Par exemple, le climat est certes gouverné par des institutions sur un schéma multi-niveau, mais aucune d'entre elle n'a « *des moyens de surveillance ni des pouvoirs de sanction (...) capables de garantir l'intégrité de la reproduction de la ressource partagée* », ce qui fait

⁴²⁵ HARDIN Garrett, « The Tragedy of the Commons », *Science*, vol. 162, 1968, p. 1243-1248

⁴²⁶ OSTROM Elinor, *Governing the Commons : The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990

⁴²⁷ CORIAT Benjamin, « Biens communs (approche économique) » in CORNU M., ORSI F., ROCHFELD J. (dir.), *Dictionnaire des biens communs*, 2017, préc., p. 99

du climat un bien commun. Le bien commun devient un commun lorsqu'il acquière une gouvernance capable de préserver ses ressources contre la tragédie des communs. On verra que le réseau internet est un commun, en ce sens que de nombreux acteurs (opérateurs, administrateurs d'applications, législateurs...) contribuent à la régulation d'internet dans le cadre d'une organisation multi-niveaux, de manière à préserver internet contre sa disparition.

Pour le moment, on s'intéresse seulement à la nature du code binaire en tant que bien commun de fait. Ce bien commun irrigue la totalité du cyberspace. **On définit le cyberspace comme l'ensemble des mémoires informatiques** (mémoires vives, mémoires mortes, disques durs internes et externes, clés USB, cartes mémoires...) **connectées à internet**. Cette définition permet d'évaluer très exactement la superficie du cyberspace, en additionnant les capacités de toutes les mémoires connectées à internet⁴²⁸. Or, on a vu que ces mémoires contiennent exclusivement des données binaires, de manière que le cyberspace est composé de code binaire et de rien d'autre. Dès lors que le cyberspace est entièrement constitué par un bien commun, **son contenu dépend des actions des différents prescripteurs numériques**. Le cyberspace est donc nécessairement co-construit par tous les prescripteurs numériques, sans qu'une catégorie de prescripteurs puisse être négligée dans cette construction⁴²⁹.

En tant que cet espace est construit au moyen de *prescriptions*, on dira du cyberspace qu'il constitue une *réalité prescriptive*. À notre connaissance, ce concept de réalité prescriptive nous est propre. On identifie une réalité prescriptive à partir de trois conditions cumulatives : (i) l'existence de prescriptions ; (ii) l'existence d'un mode prescriptif propre, *i.e.* un mode de production, d'exécution et d'ordonnancement propres aux prescriptions identifiées dans la première condition ; (iii) et l'existence d'un espace (matériel ou immatériel) dans lequel ces prescriptions peuvent exister concrètement.

Les prescriptions comptent parmi les ingrédients basiques d'une organisation sociale⁴³⁰, mais ces prescriptions n'ont pas toujours appartenu aux mêmes ensembles. Aujourd'hui, l'« ensemble » de prescriptions que nous, juristes, maîtrisons le mieux est encore l'État. Tel n'a pas toujours été le cas : avant les États, les « ensembles prescriptifs » dominants se nichaient dans les empires, les institutions religieuses et les fiefs féodaux. À la différence de l'État (limité par des frontières, régi par l'égalité souveraine), l'Empire poursuit une vocation universelle (il est censé couvrir le monde connu). Cette différence suffit à confier aux prescriptions des caractéristiques *fondamentalement* différentes selon que ces prescriptions sont issues d'un Empire ou d'un État : la portée des prescriptions étatiques se heurtera aux conditions territoriales de l'État délimité par des frontières, tandis que la frontière est une condition très relative (voire déniée) dans la portée des prescriptions impériales. Le mode prescriptif impérial inspire davantage de comportements conquérants, tandis que le mode prescriptif étatique impose la limite pacificatrice des frontières (à l'origine d'autres conflits cela dit). L'espace

⁴²⁸ Pour prendre un exemple purement fictif, on peut imaginer que la superficie du cyberspace est de 1000 quettaoctets (soit 10 000³⁰ octets)

⁴²⁹ On verra ainsi plus loin que tous les prescripteurs numériques peuvent concrètement contourner les techniques de régulation mises en oeuvre, qu'ils peuvent le faire quelles que soient les techniques employées, et que le concours de chaque type de prescripteurs est nécessaire pour garantir l'efficacité de la régulation sur internet.

⁴³⁰ On le verra plus loin avec la théorie de la régulation sociale proposée par le sociologue Jean-Daniel Reynaud

d'existence des prescriptions n'est pas le même pour l'État (territoire géographique délimité par des frontières) et pour l'Empire (territoire géographique non délimité par des frontières).

Du mode prescriptif étatique découlent des conséquences tentaculaires qui n'auraient pas pu voir le jour dans un Empire : dans un espace de conquêtes impériales, n'aurait sans doute pas existé la règle fondamentale en droit des étrangers selon laquelle toute personne victime de persécutions doit pouvoir trouver refuge dans un État et obtenir un statut protecteur⁴³¹. N'aurait sans doute pas non plus existé la règle selon laquelle tout être humain doit trouver une protection juridique auprès d'un ordre étatique⁴³². En effet, ces règles résultent des principes du droit international d'égalité, de reconnaissance et de respect mutuels que se doivent les États en qualité d'entités autonomes. Or, ces principes qui reposent sur la distinction territoriale des États sont peu compatibles avec le mode prescriptif impérial qui ignore les frontières et inspire la conquête prescriptive internationale.

De la même façon, les Églises ou analogues (Synagogues, Mosquées, Pagodes...) jouent le rôle d'« exécutantes » des prescriptions spirituelles⁴³³, équivalant à celui des institutions étatiques (juge, législateur, administration) pour ce qui est de l'État. Seulement, les prescriptions religieuses ne suivent pas le même mode de production, ni le même mode d'exécution que les prescriptions étatiques, et partagent encore moins le même espace. Comme pour l'Empire, la portée des prescriptions religieuses ne connaît théoriquement pas de frontières ; contrairement à l'Empire, le champ d'application des prescriptions religieuses ne porte pas sur un territoire géographique mais immatériel, « spirituel ». Nous n'incluons dans la réalité religieuse que le mode prescriptif décrit, à savoir des prescriptions produites par les personnes légitimes au nom des textes fondateurs, exécutées selon un mode institutionnel ecclésiastique, et donnant naissance à un mode d'ordonnancement propre. Nous excluons donc de cette réalité prescriptive les opinions d'un croyant : (a) si elles n'ont pas été produites par quelqu'un ou quelque chose reconnu par les principes fondamentaux de cette religion comme faisant autorité ; (b) si elles n'ont pas été exécutées selon le mode institutionnel identifié ; (c) ou si elles ne sont pas soumises aux règles d'ordonnancement identifiées.

Au moyen de leur exécution, les prescriptions sont validées dans leur caractère contraignant (que cette contrainte soit coercitive par le recours à la force physique ou non) ; au moyen des règles d'ordonnancement, les prescriptions peuvent interagir entre elles et maintenir la réalité prescriptive « en vie », sauvegarder son évolution dynamique ; au moyen de leur espace de déploiement, les prescriptions conservent leur existence. Ces critères nous semblent ceux pertinents pour identifier un ensemble de prescriptions comme appartenant à une même unité assurant sa propre existence⁴³⁴. On parle de « réalités » prescriptives parce que ces ensembles prescriptifs forment leur propre réalité, se réalisent eux-mêmes.

⁴³¹ Convention de Genève de 1951

⁴³² Interdiction de l'apatridie par la Convention de New York de 1961 et la convention européenne sur la nationalité de 1997

⁴³³ Sur le concept de « *prescriptions religieuses* », v. le point de vue de CARBONNIER Jean, « La religion, fondement du droit ? » in *Droit et religion*, Archives de Philosophie du Droit, tome 38, Sirey, 1993, p. 17-21

⁴³⁴ René Carré de Malberg disait de l'Etat qu'il « *s'appartient à lui-même* », raison pour laquelle il lui reconnaissait une volonté propre et en concluait l'existence d'une puissance publique distincte des subjectivités : CARRÉ DE MALBERG René, *Contribution à la Théorie générale de l'État*, Dalloz, 2004, p. 169s.

Les réalités prescriptives changent l'orientation de la société, comme on a pu l'illustrer avec le passage de l'Empire à l'État. Les périodes de l'histoire sont marquées par des successions de réalités prescriptives. Schématiquement, dans le Bas-Moyen Âge, les réalités prescriptives dominantes étaient les réalités impériale, religieuse et féodale (qui suit un mode prescriptif contractualiste au sens du droit privé). Aujourd'hui, les réalités prescriptives dominantes semblent être les réalités étatique, numérique et économique⁴³⁵.

Chaque réalité prescriptive possède ses propres conditions d'existence, est *constituée* par ces conditions d'existence. On définira ici la constitution, au-delà de sa signification juridique, comme l'ensemble des éléments qui conditionne l'homogénéité nécessaire à l'existence d'une chose ainsi constituée. Par exemple, la science du droit a découvert deux types de conditions auxquels l'ordre juridico-étatique doit son autonomie existentielle : des conditions formelles (la Constitution est identifiée selon sa place dans la hiérarchie des normes, selon son support, selon ses procédures ou circonstances de création...) ; et des conditions matérielles (la Constitution est identifiée selon les principes fondamentaux qu'elle comporte, selon son objet institutionnel ou politique, selon sa force matricielle dans l'ordre juridique...). On a démontré de même que, pour la réalité prescriptive numérique, les modes de production (ouvert et égalitaire), d'exécution (inaltéré et aliénant) et d'ordonnancement (ubiquitaire et diffusible) doivent leur existence aux lois internes à la machine (lois de neutralité exécutive, d'interopérabilité exécutive et de solidarité applicative) et au réseau (lois d'interconnexion binaire, protocolaire et opérationnelle). Dans la mesure où ces lois conditionnent le mode prescriptif numérique, on peut considérer qu'elles intègrent la constitution de la réalité prescriptive numérique.

Les comportements humains se situent au carrefour de ces diverses réalités prescriptives. Les êtres humains sont aujourd'hui soumis, notamment, aux prescriptions sociales⁴³⁶, étatiques, numériques, économiques et religieuses. Il en découle que la régulation des comportements humains dépend de plusieurs réalités prescriptives, et non d'une seule. Plutôt que de se disputer leur influence sur les comportements humains, on pense donc préférable que ces réalités prescriptives se coordonnent pour éliminer les comportements jugés problématiques. Cette analyse se rapproche de la théorie de Gunther Teubner, pour qui la société est composée de « *grands domaines sociaux* » porteurs de « *fragments constitutionnels* » dont l'assemblage formerait l'organisation sociale dans son ensemble⁴³⁷. À défaut d'une telle coordination, le droit étatique sera condamné à l'inefficacité, car l'existence et l'ordonnancement de ces réalités ne sont tout simplement pas de son ressort. On en déduit que, comme toute réalité prescriptive, l'État est autonome dans son existence mais hétéronome dans ses actions (car contraint par les autres réalités prescriptives).

Pour conclure, la considération que le code binaire est la source de la contrainte endogène implique : le dépassement des programmeurs comme seule source de contrainte pour la compréhension et l'exécution machinales, et l'identification des autres prescripteurs

⁴³⁵ La réalité prescriptive économique est concrétisée par les flux de capitaux, et son espace de déploiement est mondial. V. notamment ROBÉ Jean-Philippe, « Globalization and Constitutionalization of the World Power System », in ROBÉ J.-P., LYON-CAEN Antoine et VERNAC Stéphane (dir.), *Multinationals and the Constitutionalization of the World Power System*, Routledge, 2016, p. 11-52

⁴³⁶ V. La théorie de la régulation sociale de Jean-Daniel Reynaud, *infra*

⁴³⁷ TEUBNER Gunther, *Fragments constitutionnels. Le constitutionnalisme sociétal à l'ère de la globalisation*, Classiques Garnier, 2016

numériques ; ainsi que la reconnaissance du cyberspace comme une réalité prescriptive et un bien commun, de ce fait construit collectivement par les prescripteurs numériques, interdépendants. Après avoir approfondi le fonctionnement et la nature de notre objet d'étude, on peut à présent s'interroger sur la régulation la plus efficace compte tenu de ce fonctionnement et de cette nature (Partie 2).

DEUXIÈME PARTIE – LA RÉGULATION DES RAPPORTS DE FORCE INTERHUMAINS EN LIGNE

On a vu dans la Première Partie les différentes perspectives scientifiques proposées pour expliquer les rapports de force interhumains en ligne. On a tenté de les compléter par notre théorie des prescriptions numériques, selon laquelle les rapports de force interhumains qui se produisent dans le cyberspace naissent d'une production de données binaires assortie d'une instruction en langage machine (instruction préalable ou instruction machine). On a vu à cette occasion que toute donnée binaire n'est pas *per se* une prescription numérique : les données d'adresse et de caractère ne constituent pas en elles-mêmes de telles prescriptions car elles ne prescrivent aucune règle exécutable ; elles sont toutefois incluses dans une prescription numérique dès qu'elles sont assorties d'une instruction (ce qui est systématiquement le cas en pratique, car aucun caractère ni adresse n'est ignoré par les instructions stockées dans la machine).

Par conséquent, le cyberspace possède un mode prescriptif dont on a rapporté les particularités, qui en font une « réalité prescriptive » à part entière. Obéissant à des règles qui lui sont propres, cette réalité prescriptive confère à tous les êtres humains qui produisent des données binaires en ligne les pouvoirs, notamment : de contraindre à distance des machines numériques à exécuter des requêtes et à les appliquer d'une manière *identiquement* conforme aux règles dont l'exécution est requise ; de diffuser leurs données à très grande échelle, du fait de leur constante disponibilité à être exécutables par n'importe quelle machine connectée à internet ; et d'exercer ces capacités sans que ces dernières puissent être appropriées. En découle une interdépendance assez forte entre les prescripteurs numériques qu'on a identifiés, et donc la nécessaire coopération de ces différents prescripteurs pour réguler efficacement le cyberspace. La connaissance des catégories de prescripteurs numériques nous permet alors de savoir les catégories d'êtres humains dont la coopération est requise pour réguler efficacement l'échelle de diffusion d'une donnée.

Dans cette Deuxième Partie, on démontrera et on illustrera cette nécessaire coopération pour la régulation du cyberspace, et on tentera de répondre à la question : comment obtenir la coopération des prescripteurs numériques pour que soit respectée une norme juridique ? Cette partie sera exclusivement consacrée, non à l'étude scientifique des rapports de force interhumains en ligne mais à leur régulation. On présentera dans un premier temps les bases de la régulation de ces rapports de force (**Sous-Partie 1**). Dans un second temps, on évaluera l'efficacité des techniques de régulation et on proposera un modèle théorique pour contrôler efficacement l'échelle de diffusion d'une donnée en ligne (**Sous-Partie 2**).

Sous-Partie 1. Techniques basiques de restriction de l'accès à internet

Le concept de *régulation* connaît un succès scientifique certain depuis la seconde guerre mondiale. Il a pour originalité de traverser presque toutes les disciplines scientifiques, d'être un concept transdisciplinaire à l'instar du concept de *système*. Plus qu'un concept, la régulation désigne avant tout une méthode scientifique pour résoudre un problème comme on le verra. L'étude approfondie de cette méthode a même donné lieu à une science dédiée à la régulation - la cybernétique.

La compréhension des étapes constitutives de la méthode régulatoire est d'abord nécessaire pour savoir comment l'appliquer à internet. On questionnera ici, non la régulation du réseau

internet en général, mais la régulation de l'échelle de diffusion d'une donnée dans le cyberspace. Seront donc étudiées diverses techniques de régulation de cette échelle de diffusion. Cette Sous-Partie 1 se consacre à l'étude d'un type de techniques de régulation : les techniques restreignant l'accès à une donnée (techniques de restriction). On exposera à ce titre les critères dont on se sert pour distinguer les techniques de restriction.

L'examen du concept de « régulation juridique de l'échelle de diffusion » et de nos critères de distinction entre les techniques de restriction fera l'objet du premier temps de l'analyse (**Chapitre 1**). Ces critères seront illustrés par les techniques de suppression de données, de chiffrement, et d'avertissement précédant l'accès à des données. En second lieu, on décrira les avantages et inconvénients de deux techniques de restriction aujourd'hui privilégiées par les États pour contrôler l'échelle de diffusion d'une donnée : le blocage et le filtrage (**Chapitre 2**).

Chapitre 1. Introduction à la régulation d'internet

On détaillera d'abord l'évolution du terme *régulation* et de sa signification, ce en quoi consiste cette méthode et les concepts personnels qu'on mobilisera pour évaluer l'efficacité de la régulation sur l'échelle de diffusion d'une donnée (Section 1). Pour illustrer notre définition d'une telle régulation, seront ensuite exposés certaines techniques de restriction déployées par des normes juridiques, et surtout les critères à partir desquels on distingue les techniques de régulation échantillonnées dans cette thèse (Section 2).

Section 1. La régulation juridico-étatique d'internet

Après examen des concepts-clés qui fondent la méthode régulatrice (Paragraphe 1), on les appliquera à la régulation juridique de l'échelle de diffusion d'une donnée dans le cyberspace pour délimiter le cadre de la méthode employée ici et pour mesurer l'efficacité ou l'inefficacité de la régulation juridique en la matière (Paragraphe 2).

Paragraphe 1 – Les bases du concept de régulation juridique

On s'appuie sur l'histoire de la régulation pour en tirer une définition générale (A), puis on débute l'étude de la régulation juridique à partir de ses antécédents historiques (B).

A) Introduction au concept de régulation

1. Histoire scientifique de la régulation

Le mot *régulateur* (popularisé avant le mot *régulation*) a conservé une définition assez stable dans les disciplines scientifiques depuis le XVIII^e siècle en France. Il est d'abord utilisé dans le domaine mécanique pour désigner (vers 1728) le pendule de l'horloge à balancier inventé en 1656 par Christiaan Huygens et Salomon Coster, puis le « ressort régulateur » chargé de ramener le pendule à son point d'équilibre⁴³⁸. Il désigne aussi, à la même période, le régulateur à laminage

438HUYGENS Christiaan, *Œuvres complètes de Christiaan Huygens. L'horloge à pendule ou à balancier de 1666 à 1695*, Société hollandaise des sciences, Martinus Nijhoff, 1934, p. 502s. V. aussi : « pour ce qui est des deux manières de composer la Puissance réglante dans les Montres de Poches (...), la deuxième manière de régulation (...) est aussi par un Balancier, qui diffère de l'autre principalement en ce qu'il est plus large & plus pesant, & par conséquent moins influé par les irrégularitez du rouage, & que d'ailleurs il est aidé dans ses vibrations par un Ressort spiral d'acier, qui contribue merveilleusement à la justesse de ses mouvemens. Cette manière de régulation est

de plomb (un dispositif technique qui permet de contrôler mécaniquement les mouvements d'un cylindre pour laminier le plomb sur un deuxième cylindre placé en-dessous du premier)⁴³⁹, les régulateurs des pompes foulantes et aspirantes (mécanismes qui assurent l'entrée et la sortie de l'air pour surélever le niveau d'eau)⁴⁴⁰, le régulateur de la charrue (mécanisme qui assure l'équilibre de la charrue)⁴⁴¹, puis le régulateur de Watt à la fin du XVIIIe siècle (mécanisme qui automatise la fermeture de la vanne de la machine à vapeur en cas de forte combustion afin de diminuer l'admission de vapeur, et l'ouverture la vanne en cas de faible combustion afin d'augmenter l'admission de vapeur).

Sous l'influence de cette atmosphère mécanique du XVIIIe siècle, et de la philosophie mécaniciste de René Descartes qui explique toutes les actions par des lois physiques, automatiques et mécaniques, les révolutionnaires français emploient le terme *régulateur* comme synonyme de contre-pouvoir institution dans le cadre de l'équilibre des pouvoirs publics⁴⁴². C'est un premier glissement de sens : le *régulateur* quitte les champs mécaniques, mathématiques et géométriques pour intégrer le champ politique et institutionnel. Il faudra attendre le XIXe siècle pour que le mot *régulateur* imprègne toutes les disciplines scientifiques – la biologie (via le système nerveux régulateur décrit par Claude Bernard)⁴⁴³, l'électricité (via le télégraphe

présentement devenu universelle, & la seule qui soit en usage [depuis plus de 40 ans] » (SULLY Henri, Règle artificielle du temps, G. Dupuis, 1737, p. 43)

439Dispositif rapporté par l'historien DE SAINT ALBINE Pierre-Raymond, *Mémoire sur le laminage du plomb*, Imprimerie de Pierre Prault, 1731, p. 2-4

440DESAGULIERS Jean-Théophile, *Cours de physique expérimentale*, Tome 2, J. Rollin, 1751 [le cours cité a été publié en 1727], p. 471s.

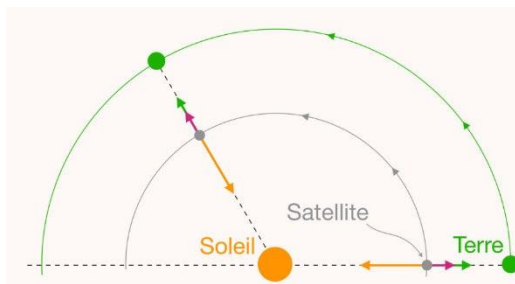
441DUHAMEL DU MONCEAU Henri-Louis, *Éléments d'agriculture*, Tome 2, H. L. Guérin et L. F. Delatour, 1762, p. 6

442On a vu que Nicolas de Condorcet était particulièrement influencé par la mécanique, lorsqu'il revendiquait un « roi automate ». On verra plus loin que, durant les débats révolutionnaires, les députés Isaac Le Chapelier, le duc de la Rochefoucauld ou encore Pierre-Louis Rœderer emploient le terme *régulateur* comme synonyme de contre-pouvoir (la deuxième chambre devrait être le « *régulateur* » des « *décisions précipitées* » de l'Assemblée Nationale pour la Rochefoucauld, le corps législatif devrait être le « *régulateur de la Cour de cassation* » pour Le Chapelier, l'administration fiscale devrait être le « *régulateur du pouvoir exécutif* » pour Rœderer)

443BERNARD Claude, *Rapport sur les progrès et la marche de la physiologie générale en France*, Imprimerie impériale, 1867 : « *Quand on accélérât la circulation capillaire, on voyait la chaleur des parties augmenter, la sensibilité s'exalter et les sécrétions apparaître avec plus de force. Quand, au contraire, sous l'influence du système nerveux, la circulation diminuait ou s'arrêter, la sensibilité s'éteignait et les éléments organiques cessaient de fonctionner. (...) Bien que le cœur soit l'organe moteur unique de la circulation générale, le système nerveux sympathique, en agissant sur la contractilité des petites artères, devient le régulateur de la circulation capillaire* » (p. 65) ; « *Le nerf est un (...) régulateur des phénomènes : il agit sur les vaisseaux de l'organe, les resserre ou les dilate, active ou ralentit le cours du sang, restreint ou prolonge la durée des contacts entre le sang et les éléments histologiques du tissu, et augmente ou diminue par cela l'énergie des échanges et des mutations physico-chimiques* » (p. 90)

puis le circuit électrique)⁴⁴⁴, l'économie (via les notions d'État régulateur, de prix régulateur et de régulation du marché par la concurrence et par la relation offre/demande)⁴⁴⁵, et la sociologie⁴⁴⁶.

Entre la deuxième moitié du XIXe siècle et la première moitié du XXe siècle, les scientifiques rapportent la régulation au concept d'équilibre. Le concept d'équilibre est parfaitement illustré par les travaux de Leonhard Euler et Joseph-Louis Lagrange au XVIIIe siècle. En 1772, ces deux mathématiciens recherchent les positions dans lesquelles un satellite peut être en équilibre dans l'espace extra-atmosphérique. En effet, un satellite placé entre la Terre et le Soleil subira l'opposition entre la force d'attraction du Soleil (le satellite est attiré vers le Soleil) et la force d'attraction de la Terre (la satellite est en même temps attiré vers la Terre), en plus de subir son propre effet centrifuge (effet qui tire le corps vers l'extérieur, tel le conducteur d'une voiture dans un rond-point). Cependant, si le satellite est placé à une certaine distance entre la Terre et le Soleil, ces trois forces se compensent et le satellite est alors en équilibre. Pour rester à l'équilibre, le satellite doit tourner autour du Soleil à la même vitesse que le fait la Terre. Il maintiendra alors systématiquement la même distance entre le Soleil et la Terre, et conservera ainsi son équilibre malgré la rotation



⁴⁴⁴ Le télégraphe possède en effet un composant rectangulaire appelé « régulateur » conçu pour retranscrire les signaux émis par deux autres composants – les indicateurs – en décrivant, à l'aide un axe rotatif, des cercles de diamètre distinct selon le signal reçu (CHAPPE Ignace Urbain Jean, *Histoire de la télégraphie*, Ch. Richelet, 1840, p. 76s. ; Abbé MOIGNO, *Traité de télégraphie électrique*, Vol. 1, A. Franck, 1852). Pour l'application aux dispositifs qui ouvrent et ferment le passage du courant électrique, v. GUEBHARD Alfred, *De la lumière électrique*, L. Hachette et Cie, 1867, p. 18s.

⁴⁴⁵ « Sous [s'adressant au journaliste socialiste Louis Blanc] répondez que l'État sera un meilleur régulateur du marché que la concurrence ; mais vous ne prouvez pas, et trouvez bon que nous ne changions pas encore de conviction », (GARNIER Joseph, « Organisation du travail, par M. Louis Blanc » *Journal des Économistes*, Vol. 11, 1845, p. 426) ; « la concurrence agit comme régulateur du prix et de la quantité des produits » (LE HARDY DE BEAULIEU Charles, *Traité élémentaire d'économie politique*, A. Lacroix, 1861, p. 78) ; « la loi universelle en économie politique, c'est (...) que le rapport entre la demande et l'offre est le régulateur unique de la valeur » (RICHELOT Henri, *Un révolution en économie politique*, Capelle, 1863, p. 50) ; le développement de la concurrence sur les marchés de céréales a eu pour conséquence « d'établir sur [ces] marchés (...) un prix à la fois régulateur et impersonnel, résultant uniquement des quantités disponibles pour la vente » (DE MOLINARI Gustave, *Les bourses du travail*, Guillaumin, 1893, p. 111)

⁴⁴⁶ Dans les années 1850, le philosophe et sociologue Auguste Comte use et abuse des termes régulateur/régularisé/réglé dans des contextes biologiques pour conceptualiser le fonctionnement de l'organisme (D'HOMBRES Emmanuel, « Compréhension et extension du concept de régulation en sociologie et en science politique à la lumière des enseignements de la biologie », in *La régulation entre sciences de la vie et sciences du gouvernement (XIXe-XXe siècles)*, Revue Arabes, n° 4, 2008, p. 31). En 1873, le sociologue Herbert Spencer interroge : « n'est-il pas probable que ce qui dans l'organisme individuel est improprement (...) appelé vis medicatrix naturae, ait son analogue dans l'organisme social ? » (SPENCER Herbert, *The Study of Sociology*, London, H. King & Co, 1873, Chap. I, p. 16). En poussant cette métaphore un peu trop loin et un peu trop approximativement, H. Spencer considère l'État comme un régulateur (« organe régulateur », « agent régulateur », « système régulateur », « appareil régulateur »...) de l'organisme social

de la Terre autour du Soleil. Le point d'équilibre du satellite est alors le point à l'endroit duquel les forces physiques se compensent⁴⁴⁷.

On définit ainsi le point d'équilibre comme le point à l'endroit duquel des effets contraires se compensent ⁴⁴⁸. Lorsque les scientifiques de la deuxième moitié du XIXe recherchent des équilibres, ils ne font rien d'autre que rechercher le(s) point(s) où se compensent des effets contraires : en économie, l'offre et la demande (effets contraires de la production et de la consommation) se compensent là où il y a autant d'offre que de demande, auquel cas le marché est équilibré ; en biologie, l'absorption et l'élimination (effets contraires) d'une substance toxique par l'organisme se compensent là où il y a autant d'élimination que d'absorption d'une substance toxique, auquel cas la santé de l'organisme est équilibrée⁴⁴⁹ etc.

Quant aux chercheurs de la première moitié du XXe siècle, ils approfondissent particulièrement la relation entre *régulation*, *équilibre* et *système* ⁴⁵⁰. Deux courants scientifiques se spécialiseront dans l'étude de cette relation tripartite : la théorie générale des systèmes (TGS) ; et surtout la cybernétique. Initiée par le biologiste Ludwig von Bertalanffy en 1937, la TGS est un projet interdisciplinaire qui consiste à identifier la notion et les implications d'un *système* dans les différentes sciences (physique, mathématiques, économie, neurosciences, médecine, sociologie, sciences linguistiques, sciences politiques, ingénierie...). Dans sa définition complète par

⁴⁴⁷ Nos connaissances sur les points de Lagrange, et le schéma pour les illustrer, sont principalement issus de RAMOND Paul (post-doctorant en astro-physique), « Satellites : l'importance des "points de Lagrange" », *Polytechnique insights* [Revue de l'Institut Polytechnique de Paris, en ligne], 1er juin 2022

⁴⁴⁸ On préfère le terme « effets » contraires à celui de « forces » contraires. Cette préférence s'explique par le fait qu'une force est la cause d'un effet ; des forces ne se contredisent pas concrètement par elles-mêmes, mais par les effets qu'elles provoquent. Ainsi, il est depuis longtemps admis en sciences physiques que l'effet centrifuge n'est pas une force, mais un effet qui résulte de plusieurs causes. De même, à travers sa théorie de l'espace-temps, Albert Einstein démontre que la gravitation n'est pas une force mais un effet qui se traduit par une courbure de l'espace : « *les trois dimensions de l'espace – la longueur, la largeur et la hauteur – sont liées à une quatrième dimension – le temps. C'est ce qu'on appelle en physique l'espace-temps. "On peut imaginer l'espace-temps comme une grande toile tendue. Si on pose un objet massif au milieu, il creuse cette toile. Si on y ajoute un deuxième objet plus petit, il se déplacera vers l'objet le plus lourd [il sera attiré vers ce dernier]. C'est selon ce principe que fonctionne la gravité [c'est-à-dire l'attraction terrestre]"* » (Arte, « Comment voyager dans le temps », interview de la physicienne Saskia Grunau vers 10 minutes, podcast du 9 mai 2023).

⁴⁴⁹ BERNARD C., *Rapport sur les progrès et la marche de la physiologie générale en France*, préc., Imprimerie impériale, 1867 : « *Quand on veut juger de l'absorption des substances par leurs effets toxiques, il est (...) très important de tenir compte de la relation ou plutôt de l'équilibre qui peut s'établir entre l'absorption et l'élimination de la substance toxique* » (p. 198). V. aussi : « *Tous les organes sécréteurs forment par leur ensemble un système de trop-plein physiologique qui doit maintenir équilibrée la composition du sang* » (p. 207) ; « *l'atmosphère intérieure dans laquelle fonctionnent les éléments histologiques [i.e. les tissus vivants] doit, comme l'atmosphère extérieure dans laquelle vit l'organisme, se maintenir dans une constitution physico-chimique à peu près constante. Cet équilibre de composition du milieu intérieur, qui est nécessaire à l'entretien des phénomènes élémentaires de la vie, ne peut être obtenu qu'à la condition d'une rénovation et d'une épuration incessante du fluide sanguin.* » (p. 68).

⁴⁵⁰ Le lien entre ces concepts a déjà été quelques fois proposée dans la deuxième moitié du XIXe siècle (on le remarque dans les extraits déjà cités de Claude Bernard notamment), mais c'est au cours de la première moitié du XXe siècle que la réflexion scientifique se spécialise dans l'étude de cette relation tripartite.

Bertalanffy, un système est un ensemble dont les parties constitutives (i.e. les composants qui dépendent de leur appartenance à l'ensemble) **sont interactives** (système concret) **ou interreliées** (système conceptuel).⁴⁵¹ Malgré plusieurs échecs (incapacité à trouver une définition commune au système, critique d'un concept applicable à tout et donc logiquement vide...), la TGS a pour mérite d'avoir révélé une méthode analytique commune à toutes les sciences : la formation et le maintien d'un ensemble organisé sont tous considérés comme dépendants des échanges des composants de cet ensemble entre eux et avec le milieu extérieur. Par conséquent, il est possible d'influencer la formation et le maintien d'un ensemble organisé en modifiant les échanges de ses composants entre eux et avec le milieu extérieur à l'ensemble. Des partisans de la TGS estimaient que le maintien d'un système repose sur un « équilibre de flux » entre les intrants et les extrants – équilibre qu'il est possible d'influencer en contrôlant les échanges des composants de ce système entre eux et avec le milieu extérieur⁴⁵².

Cependant, pour l'essentiel, la TGS de la première moitié du XXe siècle s'est concentrée sur les échanges internes et externes des composants d'un système sans faire le lien avec un « équilibre » du système. C'est avant tout la cybernétique qui a approfondi la relation tripartite entre régulation, équilibre et système dans les années 1940⁴⁵³. La cybernétique peut être définie comme la science de la régulation⁴⁵⁴. Le père fondateur de cette science, Norbert Wiener, appuie sa démonstration sur le 2^e principe de la thermodynamique, selon lequel « *un système peut perdre spontanément de l'ordre et de la régularité, mais (...) il n'en gagne pratiquement jamais* »⁴⁵⁵. Par conséquent, au fil du temps, un système thermodynamique tend nécessairement vers l'entropie, le désordre⁴⁵⁶. Tout système étant par définition organisé, un système qui perd toute organisation n'est plus un système, il s'éteint. Wiener estime que, face au risque d'extinction posé par le deuxième principe de la thermodynamique, un système vivant ne peut survivre qu'en s'adaptant à l'évolution du milieu extérieur. La survie d'un système vivant dépend d'un équilibre adaptabilité du système / variabilité du milieu extérieur au système : si

451 VON BERTALANFFY Ludwig, « The history and status of General Systems Theory », in KLIR George (dir.), *Trends in General Systems Theory*, New York, Wiley, 1972, p. 31 ; POUVREAU David, *Une histoire de la "systémologie générale" de Ludwig von Bertalanffy*, Thèse en histoire des sciences, EHESS, 2013, p. 384s.

452 POUVREAU D., *Une histoire de la "systémologie générale" de Ludwig von Bertalanffy*, préc., p. 412

453 On note que les années 1930-1940 marquent aussi l'apparition, en économie, du concept explicite d'« *autorégulation du marché* » sous la plume de Raymond Aron et surtout de Karl Polanyi, précisément dans le cas de Polanyi pour contester une telle capacité d'autorégulation du marché (ARON Raymond, « Monnaie et crédit », *Thalès*, vol. 4, 1937, p. 235-253 ; POLANYI Karl, *La Grande Transformations – Aux origines politiques et économiques de notre temps*, Gallimard, 1944).

454 En 1947, dans le titre original de son livre phare, Norbert Wiener définit la cybernétique comme la science « *du contrôle et de la communication chez l'animal et la machine* ». Le professeur de mathématiques du MIT explique avoir choisi le mot *cybernétique* à partir du mot grec *kubernêtikê* (κυβερνητική) issu du verbe *kubernân* qui signifie *gouverner* : « *son nom signifie l'art du pilote ou du timonier. Notons que le mot GOVERNOR qui désigne le régulateur d'une machine a été formé simplement par latinisation du mot grec qui désigne le timonier* » : WIENER N., *Cybernétique et société*, Paris, Deux Rives, 1952, p. 21

455 *Ibid.*, p. 19

456 Un système thermodynamique peut être défini comme une partie de l'Univers (gouttes d'eau présentes dans la vapeur, semelle d'une chaussure, étoile ou groupement d'étoiles...) dont l'étude isolée révèle des échanges d'énergie et/ou de matière avec le milieu extérieur à ce système (i.e. avec le reste de l'Univers).

un système vivant tombe en-dessous d'un certain niveau d'adaptabilité par rapport à la variabilité du milieu extérieur, ce système est menacé d'extinction⁴⁵⁷.

Selon Wiener, un système ne peut continuer à s'adapter qu'à l'aide de la communication, i.e. l'échange d'informations⁴⁵⁸. Un exemple typique de la manière dont la communication préserve l'organisme vivant de l'extinction est l'exemple de l'échange d'informations entre les synapses, puis entre les synapses et le système nerveux, puis entre le système nerveux et les organes. Lorsque ces communications cessent, l'organisme vivant meurt. S'effondrant dans l'entropie par défaut de communication, le système s'éteint, ne parvient plus à s'adapter à son environnement extérieur. Pour démontrer l'influence de la communication sur l'adaptabilité d'un organisme, Wiener prend l'exemple de la fourmi – un organisme rudimentaire dont les lacunes de communication interne (mode d'oxygénation très limité du cerveau, circulation médiocre du sang, pertes de mémoire à l'issue des mues, faible complexité du système nerveux...) en font des êtres « *stupidés* », condamnés à un rôle robotique, incapables d'apprendre à quitter leur fonction sociale définie à la naissance –, qu'il oppose à l'être humain – un organisme complexe dont les puissantes facultés de communication lui garantissent une forte adaptabilité à leur environnement extérieur⁴⁵⁹. Cette démonstration sur le rôle de la communication dans le maintien d'un système amène Wiener à la conclusion que « *la nature des communautés sociales dépend, dans une large mesure, de leurs modes intrinsèques de communication* »⁴⁶⁰. En somme, **dans la cybernétique, la régulation a pour fonction de garantir l'équilibre adaptabilité du système / variabilité du milieu extérieur en contrôlant les échanges qui se produisent au sein du système et avec le milieu extérieur** – sachant que Wiener s'intéresse au rôle joué par un type spécifique d'interactions (l'échange d'informations) sur cet équilibre.

La TGS et la cybernétique ont bouleversé la méthode d'analyse en psychologie, en neurosciences mais aussi en sociologie. À partir des années 1970, la sociologie abandonne

457Ibid., p. 77 : « *la survivance de la race dépend d'un équilibre d'échanges favorables entre la mutabilité et l'adaptabilité à diverses conditions, et entre la variabilité du milieu où la race doit exister* » ; « *une collectivité permanente qui tombe au-dessous d'un certain niveau cesse (...) par-là d'être stable* ». Wiener prend l'exemple des familles consanguines, qui ont progressivement provoqué leur propre extinction en transmettant l'épilepsie, la cécité et des malformations aux générations suivantes, rendant ainsi ces générations de plus en plus inaptées à s'adapter au milieu extérieur. Il prend aussi l'exemple des éléphants indiens, certes très nombreux, mais qu'il juge menacés d'extinction dès lors que leur constitution est particulièrement uniforme, et donc leur niveau de mutabilité particulièrement faible.

458Ibid., p. 161 : « *l'information est (...) le nom du contenu de notre échange avec le monde extérieur pendant que nous nous ajustons à celui-ci et que nous lui faisons subir le processus de cette adaptation* »

459WIENER N., *Cybernétique et société*, préc., Deux Rives, 1952, p. 83s. « *La camisole de force physique dans laquelle un insecte grandit est directement responsable de la camisole de force mentale qui règle le modèle de son comportement. (...) Les conditions mécaniques dans lesquelles se produit l'acte de l'insecte [sont] telles que l'intelligence de l'individu s'en trouve limitée* » (p. 91)

460WIENER N., *Cybernétique...*, Deux Rives, p. 81-82 : « *il y a de communautés comme celle des Esquimaux, dans lesquelles ne paraissent exister ni fonction de chef de clan ni beaucoup de subordination, de sorte que la base de la communauté est simplement le désir commun de survivre de la part d'individus qui travaillent dans des conditions de climat et de ravitaillement effroyables. Il y a des communautés stratifiées socialement comme celles des Indes, et dans lesquelles les rapports de communication entre deux individus sont étroitement limités et modifiés par des situations ancestrales. Il y a des communautés gouvernées par des despotes, dans lesquelles toute relation entre deux sujets devient subordonnée au rapport entre le sujet et le roi.* »

progressivement l'étude isolée d'un élément de la réalité sociale, au profit d'une étude des interactions et interdépendances qui relient les différents éléments de la réalité sociale⁴⁶¹. Ainsi, l'étude des conditions sociales et des phénomènes sociaux (mouvements sociaux, mobilité et stratification sociales, capital social, habitus...) a-t-elle peu à peu laissé place à l'étude des relations sociales. Vers la fin de années 1970-début des années 1980, émerge le courant dit de la « sociologie du conflit » qui considère que toute relation interpersonnelle procède du conflit, c'est-à-dire d'une contradiction entre deux contraintes qui s'affrontent : l'expression de soi et la compréhension de l'autre⁴⁶². Inspiré par la sociologie du conflit et par son étude menée dans les années 1950 sur les relations de travail, Jean-Daniel Reynaud publie sa « théorie de la régulation sociale » (TRS) en 1989⁴⁶³. Cette théorie propose d'adapter le concept de régulation aux spécificités des rapports sociaux : « *la notion de régulation est utilisée essentiellement dans une conception normative pour désigner l'ajustement conformément à une règle par des mécanismes de contrôle qui maintiennent constants certains paramètres ou corrigent les écarts à la norme fixée. Appliquée au système social, cette conception normative tient difficilement, car les normes sociales sont des compromis instables dont la rationalité n'est pas optimale, mais tout au plus acceptable, voire tolérée ou subie.* »⁴⁶⁴.

Précisément, dans un système social, l'agent est autonome, c'est-à-dire « *capable de construire des règles et d'y consentir* » – ce qui fait de l'agent social une variable trop changeante pour pouvoir prédire un ajustement exact de son comportement à une règle contraignante. Cela conduit J.-D. Reynaud à distinguer deux types de règles : la *règle de contrôle*, qui corrige les écarts à la norme ; et la *règle autonome*, qui découle de la capacité de l'agent à construire des règles et à y consentir. Dans ce cadre, **la régulation sociale désigne un équilibre entre le contrôle** (le fait de contraindre autrui) **et l'autonomie** (le fait pour les agents sociaux d'échapper aux injonctions voire de disputer l'hégémonie de leur pouvoir normatif). Il y a régulation sociale chaque fois qu'une règle de contrôle interagit avec une règle autonome. Or, d'après la TRS, chaque action d'un agent social est considérée comme une production de règles⁴⁶⁵. Par conséquent, **tous les rapports sociaux dépendent de l'équilibre résultant des diverses**

461CHEVALLIER Jacques, « La régulation juridique en question », *Droit et société*, n° 49, 2001, p. 828 : « *Apparu au XVIIIe siècle dans les sciences techniques (machine de Watt), puis au XIXe siècle en physiologie (Claude Bernard), le concept a connu, après la Seconde Guerre mondiale, une spectaculaire diffusion dans les sciences sociales, d'abord sous l'influence du développement de la cybernétique, puis dans le cadre de la théorie générale des systèmes. La régulation constitue un élément-clé de la théorie générale des systèmes : tout système organisé, formé d'un ensemble d'éléments interdépendants et interagissants, serait en effet en permanence confronté aux facteurs de déséquilibre et d'instabilité provenant de son environnement ; la régulation recouvre l'ensemble des processus par lesquels les systèmes cherchent à maintenir leur « état stationnaire », en annulant l'effet des perturbations extérieures. La diffusion du concept de régulation a suivi très logiquement celle de la démarche systémique dans les sciences sociales : le mode de raisonnement systémique, qui envisage chaque élément de la réalité sociale, non pas isolément, mais à travers les relations d'interdépendance et d'interaction qui l'unissent à d'autres, s'est en effet progressivement imposé dans toutes les sciences.* »

462BULLE Sylvaine et TARRAGONI Federico, *Sociologie du conflit*, Armand Colin, 2021 ; FREUND Julien, *Sociologie du conflit*, Presses Universitaires de France, 1983

463REYNAUD Jean-Daniel, *Les règles du jeu. L'action collective et la régulation sociale*, Armand Colin, 1989

464DE TERSSAC Gilbert, « La théorie de la régulation sociale : repères pour un débat » in DE TERSSAC G. (dir.), *La théorie de la régulation sociale de Jean-Daniel Reynaud*, 2003, p. 11

⁴⁶⁵ Dans la TRS, « *l'action [est] entendue comme une production de règles* » (ibid., p. 12)

régulations sociales, i.e. des interactions entre règles de contrôle et règles autonomes⁴⁶⁶. Il existe ainsi de nombreux exemples de régulations sociales : les « « réglages » [spontanés] entre les différentes dimensions de la vie sociale, de l'économie, de la politique, de la culture, mais aussi [les] réglages entre l'intégration et l'exclusion, entre la contribution et la rétribution de chacun » ; les réglages intervenant pour coordonner différents niveaux de décision, pour articuler des décisions prises en amont avec leur mise en œuvre en aval ; les « « reprises d'initiative » par un acteur qui affirme sa volonté d'entrer dans le jeu (...) pour définir ses propres règles ou pour se soustraire à tout contrôle hiérarchique » ; ou encore le partage du pouvoir entre l'État et ses entités constitutives (collectivités locales, autorités administratives indépendantes, agences de renseignement...)»⁴⁶⁷.

La régulation sociale est « une sorte de "mise au point" permanente, moins pour assurer l'équilibre du système social, que pour gérer les déséquilibres et les rendre discutables, voire acceptables. Il s'agit d'une sorte de "réparation" des failles des modes de gouvernement par le haut, (...) d'une tentative de "raccordement" entre le normatif et le normal, entre ce qui devrait être et ce qui est réellement, entre une loi et un accord collectif. Il ne s'agit pas de réguler un système préexistant pour assurer son fonctionnement conformément à des normes préétablies, mais bien de construire le système social conformément aux attentes des acteurs et aux ressources dont ils disposent pour se faire entendre »⁴⁶¹

2. Définition proposée de la régulation

Cette histoire de la régulation nous permet d'en tirer plusieurs conclusions. Premièrement, on constate que les travaux scientifiques menés depuis la deuxième moitié du XIX^e siècle n'ont pas modifié la signification du concept de *régulation*, mais l'ont précisé en identifiant : (i) le **système** (i.e. tout ensemble organisé par les échanges de ses composants entre eux et avec le milieu extérieur) comme l'**objet de la régulation** ; (ii) le **contrôle des échanges** (de matière, d'énergie, d'informations...) comme la **condition de la régulation** ; et (iii) l'**atteinte d'un point d'équilibre** comme le **moyen de la régulation**. On estime que ces travaux n'ont pas réformé la signification de *régulation*, car l'action de tous les *régulateurs* du XVIII^e siècle consistait précisément à contrôler les échanges d'un ensemble organisé pour atteindre un point d'équilibre (pendule régulateur, ressort spiral régulateur, régulateur de laminage de plomb, régulateur de Watt, le contre-pouvoir institutionnel dans le cadre de l'équilibre des pouvoirs...). Aussi, bien qu'il ait fallu attendre le XVIII^e siècle pour que le terme *régulateur* soit employé avec sa signification contemporaine, le concept moderne de régulation est en réalité applicable à de nombreux objets et théories du passé : la théorie malthusienne d'un équilibre économique accroissement démographique / disponibilité des ressources, publiée à la fin du XVIII^e siècle (1798) qui a inspiré de futures politiques de régulation démographique et de contrôle des naissances ; la théorie du médecin et alchimiste Paracelse, considéré comme le père de la pharmacologie, qui au XVI^e siècle

466BRÉCHET Jean-Pierre, « Le regard de la théorie de la régulation sociale de Jean-Daniel Reynaud », *Revue française de gestion*, n° 184, 2008, p. 16 : « la TRS considère que (...) la régulation est le fait social premier, originel, à la fois à l'échelle individuelle et à l'échelle collective »

467DE TERSAC G., « La théorie de la régulation sociale : repères pour un débat », préc., p. 12-13

468Ibid., p. 15

expliquait les maladies par un déséquilibre des éléments Air/Terre/Feu/Eau conformément aux principes de la médecine grecque antique⁴⁶⁹ ; l'horloge Al-Jazari au XIIe siècle, qui régula le débit de l'eau (horloge hydraulique)⁴⁷⁰ ; ou encore le principe *vis medicatrix naturae* (« la nature est le médecin des maladies ») énoncé par Hippocrate vers le Ve-IVe siècle av. JC, selon lequel les déséquilibres organiques se corrigent le plus souvent naturellement (en principe, l'organisme guérit lui-même la maladie sans intervention médicale). La régulation n'est donc pas un procédé nouveau. C'est un procédé qui a probablement toujours existé dans l'histoire scientifique de l'humanité.

Deuxièmement, ces considérations nous permettent de définir la **régulation** comme le **procédé qui consiste à créer des règles ou à utiliser des règles existantes** (mathématiques, physiques, mécaniques, économiques, sociales, juridiques...) **pour contrôler les échanges que les composants d'un système entretiennent entre eux et avec le milieu extérieur, de façon à orienter ce système vers un point d'équilibre**. Cette définition essaie de décrire un procédé commun à toute discipline scientifique.

Le procédé de la régulation est en effet toujours le même, et s'applique toujours au même objet : **un système traversé par des effets contraires**. Par exemple, un système formé par trois corps célestes est traversé par les effets d'attraction contraires de chacun des corps ; un organisme vivant (système biologique) est traversé par les effets contraires de la mutabilité de l'organisme et de la variabilité du milieu extérieur ; un marché de biens (système économique) est traversé par les effets contraires de l'offre (qui produit des biens) et de la demande (qui consomme des biens) ; une relation sociale (système social) est traversée par les effets contraires de l'autonomie et du contrôle...

La contradiction des effets peut perturber le système. C'est le cas si un ou plusieurs effets agissent excessivement ou insuffisamment par rapport aux effets contraires. Par exemple, si un satellite situé entre la Terre et le Soleil est positionné trop à proximité du Soleil, l'effet d'attraction du Soleil agira excessivement et celle de la Terre insuffisamment, ce qui fera se rapprocher le satellite du Soleil et perturbera donc la stabilité du système formé par les trois corps célestes. Autre exemple : sur le marché du travail, s'il y a uniquement de la demande de travail (force de travail demandée par les entreprises) sans offre de travail (force de travail fournie par les ménages), la demande agit excessivement et l'offre insuffisamment, ce qui conduit à un chômage touchant 100% de la population et perturbera donc l'activité du marché du travail au point de le rendre inactif.

La régulation cherche à atteindre un point d'équilibre, c'est-à-dire **un niveau auquel les effets contraires se compensent**. Dès lors que les perturbations résultent d'un effet excessif ou

469PLANCQ Adrien, *Contribution à l'étude des apports de Paracelse (1493-1541) dans le domaine de la santé*, Thèse en sciences pharmaceutiques, Université de Caen Normandie, 23 mars 2022, p. 44 : « Paracelse distingue la lèpre simple, la lèpre mixte et la lèpre universelle. La lèpre simple correspond au déséquilibre d'un élément. (...) Si la maladie atteint les extrémités et la face, elle est due à un déséquilibre de l'élément Terre. Si l'atteinte ne concerne que les pieds et qu'il y a présence d'un gonflement testiculaire chez l'homme c'est l'élément Eau qui est en cause. Au contraire, l'association d'une haleine fétide, d'une modification du teint et d'une perte de sensibilité concerne l'élément Air et enfin le Feu se manifestera en déséquilibre par une lèpre avec ulcères et congestion locales à type de brûlures sur le corps. La lèpre mixte est celle où au moins deux éléments sont en déséquilibre et la lèpre universelle implique que tous les éléments sont déséquilibrés. »

470EYRAUD Charles-Henri, *Horloges astronomiques au tournant du XVIIIe siècle, de l'à-peu-près à la précision*, Thèse en histoire, Université Lumière Lyon 2, p. 59

insuffisant par rapport à un effet contraire, le fait de compenser la contradiction de ces effets doit logiquement permettre d'éliminer les perturbations. En restant sur nos exemples : les effets d'attraction du Soleil et de la Terre se compensent à un endroit précis de telle manière que, si un satellite est positionné à cet endroit, le système formé par ces trois corps célestes reste stable sans subir la perturbation des effets d'attraction contraires ; de même, les effets de l'offre et de la demande de travail se compensent s'il y a autant d'offre que de demande, c'est-à-dire si offre de travail = demande de travail, auquel cas chômage = 0, et le marché du travail n'est alors plus perturbé par le chômage. Ou encore, l'organisme vivant a pour point d'équilibre le niveau auquel se compensent la mutabilité de l'organisme et la variabilité du milieu extérieur, tandis que les relations sociales ont pour point d'équilibre le niveau auquel se compensent l'autonomie et le contrôle d'après la théorie de la régulation sociale. **L'atteinte du point d'équilibre permet ainsi de corriger les perturbations qui naissent du déséquilibre entre des effets contraires.**

Or, comment orienter un système vers son point d'équilibre ? On a vu que toutes les sciences y ont apporté une même réponse : **un système peut être orienté vers son point d'équilibre en contrôlant les échanges des composants de ce système entre eux et avec le milieu extérieur.** C'est là toute la démonstration de l'exemple de la fourmi donné par Wiener : les échanges que les composants de l'organisme (cellules, synapses, système nerveux, organes...) entretiennent entre eux et avec le milieu extérieur conditionnent le point d'équilibre qui permet à la fourmi d'exister, c'est-à-dire le point d'équilibre où se compensent la mutabilité de la fourmi et la variabilité du milieu extérieur. De même, en contrôlant pleinement les échanges d'énergie et de matière des trois corps célestes (composants du système formé par les trois corps), on peut atteindre le point d'équilibre où se compensent les effets d'attraction des corps ; en contrôlant pleinement les échanges des agents économiques (composants du marché), on peut atteindre le point d'équilibre offre/demande etc.

On parle de *système autorégulé* lorsque **des mécanismes inhérents à un système contrôlent les échanges de ses composants entre eux et avec le milieu extérieur pour compenser des effets contraires qui le perturbent.** Par exemple, l'organisme de la fourmi est un système qui s'autorégule car cet organisme possède des mécanismes qui contrôlent les échanges de ses composants entre eux et avec le milieu extérieur pour compenser le déséquilibre mutabilité de l'organisme / variabilité du milieu extérieur, et ainsi pour garantir la survie de la fourmi. Ou encore, la question de savoir si le marché s'autorégule équivaut à se demander si le marché compense par-lui-même les déséquilibres offre / demande.

La régulation est un procédé aujourd'hui très prisé (par des institutions, des entreprises, des corps de métier...) pour résoudre des problèmes, probablement en raison de ses succès en mécanique, en physique, en biologie, en médecine ou encore en neurosciences. Pour la même raison, et à défaut d'avoir identifié une méthode plus efficace, on a adopté la régulation comme grille de lecture pour gouverner juridiquement les rapports de force interhumains sur internet. Pour autant, on reconnaît deux principaux défauts à la régulation. D'abord, à notre connaissance, il n'est pas démontré scientifiquement que toute perturbation d'un système provient d'un déséquilibre entre des effets contraires. En effet, si une perturbation ne provient pas d'un déséquilibre entre des effets contraires, alors le rééquilibrage de ces effets ne résoudra pas cette perturbation, et la régulation sera alors inefficace pour éliminer la perturbation problématique. Ensuite, il n'est pas non plus démontré que la régulation produit la même efficacité sur des comportements physiques, biologiques et techniques, d'une part, et sur des comportements

sociaux, d'autre part. Par conséquent, on ignore si le concept de régulation est aussi approprié en sciences sociales (économie, gestion, sciences politiques, sociologie, droit...) qu'il l'est en sciences de la nature et en sciences techniques.

B) Les antécédents de la régulation juridique en France

En sciences juridiques, la *régulation* n'a cessé de changer de significations depuis le XVIII^e siècle. On trouve des traces du mot *régulateur* dans le droit positif de l'Ancien Régime, pour désigner une administration fiscale⁴⁷¹. En ce sens, le *régulateur* qualifiait une personne qui met en œuvre la réglementation juridique, et s'inspire donc de l'ancienne signification du *régulateur* (« personne qui dirige »)⁴⁷².

On a vu qu'un premier glissement de sens juridique apparaît à la fin du XVIII^e siècle : alors que la société française rapprochait le *régulateur* du concept de régularité mécanique et non plus de réglementation juridique, les révolutionnaires français se sont imprégnés de ce contexte historique pour qualifier de « régulateurs » des institutions chargées d'arrêter mécaniquement l'abus de pouvoir⁴⁷³. Cette influence de la philosophie cartésienne sur l'esprit révolutionnaire français lègue à l'histoire du droit une approche dite « mécaniste » de la Constitution⁴⁷⁴. Par sa seule existence, la Constitution garantit le respect des droits et libertés parce qu'elle résulte de la volonté générale et définit les règles institutionnelles qui limitent les abus de pouvoir. Ainsi, en séparant les trois pouvoirs publics en trois corps distincts (exécutif, législatif, judiciaire) et en

471 Édit de Sa Majesté portant confirmation du Conseil des Commis du Duché d'Aoste du 18 janvier 1758, §22 : « nous voulons bien conserver au dit Conseil l'autorité de connaître & de punir les contraventions aux règlements faits pour la Gabelle du Sel, & la Traite foraine, en conformité des règlements par Nous approuvés (...) ; le Conseil ne pourra en vertu de cette concession, exercer aucune juridiction sur les Gabelliers, ou Fermiers, & sur le Régulateur de ladite Traite foraine, non plus que sur leurs Agens, & sur les Gardes par eux établis »

472 Par opposition à la nouvelle signification du *régulateur*, qui s'inspire de la régularité (uniformité du mouvement) plutôt que de la réglementation (domination, décision dirigeante).

473 Lors des débats sur l'établissement d'un bicamérisme ou d'un monacamérisme, le député La Rochefoucauld estimait qu'un corps unique d'adoption de la loi, « s'il n'est pas astreint à des formes précises, et si (...) il ne trouve pas un régulateur qui modère sa marche, peut mettre la nation en danger par des décisions précipitées, trop peu réfléchies, et même contraires à son vœu » (Assemblée Nationale, « Opinion de M. le duc de la Rochefoucauld sur la sanction royale », *Archives Parlementaires de la Révolution Française*, 2 sept. 1789, p. 548). De même : « ce n'est pas l'apposition d'une nouvelle moitié de tribunal à l'ancienne qui sera le régulateur de la cour de cassation ; ce régulateur sera le Corps législatif, seul et véritable interprète de la loi » (Assemblée Nationale, « Suite de la discussion sur le tribunal de cassation et adoption de six articles », Intervention du député Isaac Le Chapelier, *Archives Parlementaires de la Révolution Française*, 18 nov. 1790, p. 517). Ou encore : « Mais ce n'est pas assez, Messieurs, que le pouvoir exécutif ne puisse s'étendre par l'administration des finances au-delà des limites qui lui sont assignées ; il faut que la nation puisse arrêter et peut-être réduire ce pouvoir, dès qu'il tendra à abuser des moyens d'action et d'influence qui lui sont propres ; il faut, par exemple, qu'elle puisse sans effort, sans bruit, sans combat, anéantir une armée qui menacerait la liberté publique. Or, cette faculté dépend du pouvoir de faire cesser à l'instant la solde de cette armée. Elle tient à l'administration des finances. La finance doit donc être considérée comme le régulateur du pouvoir exécutif. Ce régulateur donc ne doit pas être à la disposition du pouvoir exécutif » (Assemblée Nationale, « Rapport par M. Rœderer sur les lois constitutionnelles des finances », *Archives Parlementaires de la Révolution Française*, 20 déc. 1790, p. 579)

474 PAPATOLIAS Apostolos, *Conception mécaniste et conception normative de la constitution*, Thèse en droit public, Sakkoulas, 2000

établissant l'existence d'une Nation (représentation des citoyens qui délèguent leur souveraineté aux députés), la Constitution empêche *mécaniquement* le despotisme (concentration abusive des trois pouvoirs), les inégalités entre citoyens (tous égaux devant la Nation) et la violation des libertés par l'État (contrôlé par la Nation)⁴⁷⁵.

Au début du XIXe siècle, les juristes appellent « régulateur » une autorité juridique regardée comme suprême pour résoudre les conflits et régler la société (loi, Constitution, Cour de cassation, Roi, État...)⁴⁷⁶. Vers la moitié du XIXe siècle, le *régulateur* est associé à un mécanisme capable de régler un système dans ses moindres détails. L'État-régulateur est alors identifié comme un État interventionniste, souvent promu par les socialistes, par opposition à un État laissant agir le libre jeu de la concurrence, généralement promu par les libéraux⁴⁷⁷. Entre la fin du XIXe siècle et les années 1950, on estime que deux phénomènes juridiques ont apporté une importante contribution à la conception moderne de la régulation : le foisonnement de droits et libertés consacrés juridiquement ; et la valeur juridique reconnue à la Constitution et au droit international. Ces deux phénomènes ont occasionné de nombreux conflits entre des droits et des principes ayant la même valeur juridique, obligeant ainsi l'État (le juge, le législateur et le gouvernement) à trouver un point d'équilibre pour concilier les droits et principes en conflit.

Concernant le premier phénomène, la fin du XIXe siècle a vu apparaître la figure de l'État libéral, c'est-à-dire d'un État garant des libertés individuelles. Cela conduit à une démultiplication des libertés publiques consacrées par la loi comme la gratuité de l'instruction (loi du 16 juin 1881), la liberté de réunion (loi du 30 juin 1881), la liberté de la presse (loi du 29 juillet 1881), la liberté d'association (loi du 1^{er} juillet 1901) et la séparation des églises et de l'État (loi du 9 décembre 1905), pour ne citer que les plus connues. La préservation des libertés ne dépend plus de la seule existence de la Nation, mais de la consécration des libertés par la loi et de leur protection par le juge. Après la seconde guerre mondiale, une nouvelle vague de droits et libertés voit le jour dans le préambule de la Constitution de 1946 instaurant la IV^e République : les droits économiques, sociaux et culturels (droit de grève et d'adhésion à un syndicat, droit d'asile, droit

⁴⁷⁵ Cela découle en partie de la théorie sieyèsienne selon laquelle la Nation est par essence garante de la volonté générale, car la Nation est une émanation de la souveraineté populaire par délégation et fait le lien entre les deux parties du pacte social (administrés et corps administratif)

⁴⁷⁶ Pour les codes juridiques : « le Code judiciaire doit être le régulateur des juges et des hommes qui se consacrent à la défense des intérêts de leurs concitoyens » (LEPAGE P. [avocat], *Nouveau style de la procédure civile dans les cours d'appel, les tribunaux de première instance, de commerce, et dans les justices de paix*, 3^e édition, Hacquart, 1807, p. xvi de la préface). Pour la loi qualifiée de « régulateur suprême », v. LOCRÉ Jean Guillaume, *Esprit du Code Napoléon*, Volume 1, Imprimerie Impériale, 1805, p. 1. Pour la Constitution : « La loi fondamentale et constitutive (...), première émanation de la souveraineté, (...) en est l'image et le représentant immédiat ; elle est le régulateur invariable de toutes les autorités, et le pacte social qui la renferme, est matériellement le registre des ordres souverains : tous les membres de la société lui doivent une égale soumission » (DAURAY DE BRIE Jean-François, *Théories des lois sociales*, Demonville, 1804, p. 60) ; « La constitution, la loi des lois, le régulateur des peuples et des rois, l'acte qui impose silence aux ambitions de toutes les époques, est la table immuable des ressorts, des axiomes sur lesquels reposent les institutions d'un empire » (MAUREL Jacques J., *Charte constitutionnelle*, Imprimerie de la veuve Gaude, 1832, p. 2). Pour la Cour de cassation, qualifiée de « régulateur de tous les tribunaux de la République » (SIREY J. B., *Du Conseil d'État selon la Charte Constitutionnelle*, préc., 1818, p. 196)

⁴⁷⁷ D'HOMBRES E., « Compréhension et extension du concept de régulation en sociologie... », *péc.*, *Araben*, n° 4, p. 33. V. aussi GARNIER Joseph, « Organisation du travail, par M. Louis Blanc », *péc.*, *Journal des Économistes*, 1845, p. 426

à la protection de la santé et à la sécurité sociale, droit d'égal accès à la culture, droit des peuples à s'administrer eux-mêmes...).

Concernant le second phénomène, les juristes commencent à reconnaître une valeur juridique à la Constitution dans les années 1930-1940, sous l'influence de Hans Kelsen. Pour conclure à la valeur juridique de la Constitution, Kelsen examine d'abord la composition du droit. On a vu dans l'Introduction que, pour Hans Kelsen, la norme désigne la signification d'un devoir-être issu d'un acte intentionnel. Cependant, cette définition est si large qu'elle inclut n'importe quel type de normes – normes religieuses, morales, professionnelles... Comment alors différencier la norme juridique de toutes les autres ?

Les positivistes de la fin du XIX^e siècle considéraient qu'une règle devenait juridique dès lors qu'elle résultait de la volonté de l'État. Cette hypothèse les conduisait toutefois à la conclusion que la Constitution n'avait pas de valeur juridique : la Constitution définit l'État, donc elle lui est nécessairement antérieure et ne peut pas résulter de sa volonté ; la Constitution résulte de la volonté populaire et, en cela, représente un fait social et non une règle juridique⁴⁷⁸. Pour distinguer les normes juridiques des autres types de normes, Kelsen procède autrement. Il commence par rassembler les normes juridiques dans un même ensemble : l'ordre juridique.

Le juriste autrichien étudie l'ordre juridique en lui prêtant les caractéristiques d'un système, c'est-à-dire d'un ensemble organisé par les échanges de ses composants. Il identifie ainsi deux façons d'organiser hiérarchiquement un ensemble de normes : les normes peuvent d'abord être hiérarchisées de manière statique (ordre statique), auquel cas le contenu des normes inférieures découle du contenu des normes supérieures ; les normes peuvent ensuite être hiérarchisées de manière dynamique (ordre dynamique), auquel cas les normes inférieures ont un contenu indépendant du contenu des normes supérieures, mais doivent se conformer aux modalités de production édictées par les normes supérieures. Les normes qui composent un ordre statique entretiennent donc un rapport hiérarchique matériel (par rapport au contenu), tandis que les normes qui composent un ordre dynamique entretiennent un rapport hiérarchique formel (par rapport aux conditions de production). « Ainsi, au système statique dans lequel les normes sont déduites les unes des autres, on opposera le système dynamique dans lequel les normes sont produites conformément les unes aux autres »⁴⁷⁹. C'est précisément ici que Kelsen situe la différence entre normes morales et religieuses, d'une part, et normes juridiques, d'autre part : tandis que la religion et la morale seraient des ordres statiques, l'ordre juridique serait un ordre dynamique.

Si Kelsen considère l'ordre juridique comme un ordre dynamique, c'est parce qu'il constate, d'une part, que le contenu du droit peut changer radicalement d'un instant à l'autre (ce qui est impossible dans un ordre purement statique) et, d'autre part, que les normes juridiques édictent les modalités de production des autres normes juridiques. En effet, la Constitution habilite le législateur à légiférer et définit les conditions d'adoption de la loi, donc édicte les modalités de production de la loi ; de même, la loi définit les capacités d'action de l'administration, de sorte qu'elle édicte les modalités de production des règlements administratifs. De là découle la

⁴⁷⁸ Ainsi, selon le positiviste René Carré de Malberg, « la constitution n'est que le produit d'une situation de fait » antérieure à l'État (CHAMPEIL-DESPLATS Véronique, « Théorie générale des sources du droit constitutionnel », in TROPER M. et CHAGNOLLAUD D. (dir.), *Traité international de droit constitutionnel*, préc., Tome 1, Dalloz, 2012, p. 244)

⁴⁷⁹ BRUNET Pierre, « Michel Troper et la "théorie" générale de l'État. État général d'une théorie », *Revue française de théorie juridique*, 2003, n° 37, p. 90-91

hiérarchie des normes selon laquelle Constitution > loi > règlement administratif. De là découle aussi l'idée selon laquelle la Constitution a une valeur juridique. En effet, le type de rapports qu'entretiennent les normes juridiques entre elles (rapports hiérarchiques par lesquels une norme définit les modalités de production d'une norme inférieure) existe également entre la Constitution et les autres normes juridiques. Du fait de son mode d'échanges avec les autres normes juridiques, la Constitution est donc une norme juridique. Elle définit les modalités de production des lois et, ce faisant, pose la condition de validité des lois – à savoir leur conformité à leurs règles de production édictées par la Constitution. De la même manière, la loi définit les modalités des règlements administratifs et, ce faisant, pose la condition de validité des règlements administratifs – à savoir leur conformité à la loi.

La théorie normativiste de Kelsen est évidemment très discutable sur deux points fondamentaux. D'abord, il a été reproché à cette théorie de mal identifier la nature des échanges entre les composants de l'ordre juridique – selon Michel Troper, l'ordre juridique serait à la fois statique et dynamique, c'est-à-dire que le contenu des normes juridiques dépend aussi largement du contenu des normes juridiques préexistantes⁴⁸⁰. Ensuite, la théorie normativiste n'identifie aucun échange entre les composants de l'ordre juridique et le milieu extérieur à l'ordre juridique – notamment les normes morales. L'ordre juridique serait un système « autarcique », exclusivement organisé par les échanges internes entre les normes qui le composent. Un tel système autarcique ne nous semble pas possible en réalité : par définition, un système est une partie de l'Univers artificiellement extraite par l'analyse humaine pour en isoler l'étude ; en-dehors de l'analyse humaine, en-dehors de cette extraction artificielle, aucun système n'est réellement séparé du reste de l'Univers, c'est une partie de l'Univers dont les composants échangent avec le milieu extérieur. Cette critique rejoint celle d'Alf Ross, pour qui la validité d'une norme juridique ne dépend pas de sa conformité à une norme supérieure mais d'un élément externe à l'ordre juridique : la perception sociale de la norme comme une norme obligatoire⁴⁸¹. Pour notre part, on considère que rien n'empêche la coexistence d'une validité formelle de la norme juridique (conformité de la norme inférieure à la norme supérieure) et d'une validité matérielle de la norme juridique (efficacité sociale de la norme).

Reste que, malgré les critiques, la théorie normativiste a fait germer l'idée que la Constitution possède une valeur juridique. Surtout, après la seconde guerre mondiale, cette théorie a fait apparaître partout en Europe des « justices constitutionnelles », *i.e.* des juridictions chargées de vérifier la conformité des lois à la Constitution. L'approche mécaniste de la Constitution a laissé place à une approche normative : les droits et libertés garantis par la Constitution n'ont plus une simple portée déclarative ; le juge en sanctionne désormais le respect. En plus des libertés publiques consacrées par l'État libéral (libertés de réunion, de la presse, d'association...), le juge doit désormais vérifier le respect des droits économiques et sociaux figurant dans le préambule de 1946 (droits de grève, d'asile, d'accès à la culture, à la protection sociale...) et des droits énoncés par la Déclaration des droits de l'Homme et du citoyen de 1789 mentionnée par la Constitution (liberté d'expression, droits de la défense, droit à la vie privée, principe de légalité pénale, liberté d'aider autrui dans un cadre humanitaire issue du principe de fraternité...). Cette

⁴⁸⁰ *Ibid.*, p. 89-90

⁴⁸¹ TROPER Michel, « Ross, Kelsen et la validité », *Droit et société*, n° 50, 2002, p. 55 : « pour Kelsen, on doit considérer qu'une norme est valide si et seulement si elle a été émise conformément à une norme supérieure, tandis que, pour Ross, elle est valide si elle est appliquée et elle est appliquée si elle est perçue comme socialement obligatoire »

démultiplication des droits et libertés, combinée à la normativité qui leur est reconnue, a pour conséquence de favoriser les occasions de conflits entre droits et libertés, obligeant ainsi le juge à faire appliquer les règles en vérifiant le respect d'un *équilibre* entre les droits et libertés en présence.

Paragraphe 2 – La régulation juridique d'internet

Sous l'influence de la « régulation » américaine, et de l'essor du concept de *régulation* depuis l'après seconde guerre mondiale, l'ordre juridique français accueille de plus en plus la méthode de la régulation pour encadrer les comportements depuis les années 1970-1980 (A). On verra comment appliquer cette méthode à internet pour contrôler l'échelle de diffusion d'une donnée dans le cyberspace (B).

A) La consécration de la régulation juridique en France

1. L'essor de la régulation juridique dans les années 1970-1980 en France

L'après-seconde guerre assiste à l'essor de la figure de l'État-providence en France qui, se reconnaissant le rôle de maintenir la cohésion sociale, intervient directement et de façon permanente dans la vie sociale en utilisant le droit comme instrument pour réaliser des objectifs de politique publique. L'instrumentalisation du droit pour servir des objectifs de politique publique a été lue rétrospectivement comme une forme de régulation juridique⁴⁸². Mais dans les années 1950-1960, la « régulation juridique » n'a pas encore ce sens. En 1962, p. ex., le Conseil constitutionnel affirme n'être qu'un « *organe régulateur de l'activité des pouvoirs publics* »⁴⁸³. En cette qualité, il ne peut pas juger le fond de la loi contestée devant lui, il peut seulement en évaluer la forme, *i.e.* vérifier que la loi a été édictée selon des procédures conformes à la Constitution. C'est la célèbre théorie du « juge aiguilleur », selon laquelle le rôle du juge constitutionnel se limite à encadrer le législateur dans sa manière d'édicter la loi⁴⁸⁴. Cette théorie a depuis été maintes fois remises en causes par la jurisprudence du Conseil constitutionnel, et le juge constitutionnel français contrôle régulièrement la conformité à la Constitution du contenu de la loi contestée devant lui⁴⁸⁵. Dans le droit positif des années 1960, le *régulateur* semblait donc être cantonné dans un contexte procédural.

482CHEVALLIER Jacques, « L'État régulateur », *Revue française d'administration publique*, n° 111, 2004, p. 473-482

483CC, Décision n° 62-20 DC du 6 nov. 1962, *Loi relative à l'élection du Président de la République au suffrage universel direct*, cons. 2

484FAVOREU Louis, « Les décisions du Conseil constitutionnel dans l'affaire des nationalisations », *RDP*, 1982, p. 419-420 ; VEDEL Georges, « Le Conseil constitutionnel, gardien du droit positif ou défenseur de la transcendance des droits de l'homme », *Pouvoirs*, n° 45, 1988, p. 151 ; VEDEL G., « Schengen et Maastricht », *RFDA*, n° 2, 1992, p. 173-184

485À commencer par la décision CC, *Loi sur l'évolution de la Nouvelle-Calédonie*, 23 août 1985, n° 85-197 DC, cons. 27 : « *la loi n'exprime la volonté générale que dans le respect de la Constitution* ». En posant pour la première fois cette affirmation, le Conseil constitutionnel juge que le législateur n'est pas souverain sur la Constitution, et que le contrôle de constitutionnalité de la loi est partie intégrante de la volonté générale. Par la suite, le Conseil constitutionnel ne cessera de vérifier régulièrement la conformité du contenu de la loi à la Constitution – bien au-delà de la procédure d'adoption de la loi.

Il faudra attendre les années 1980-1990 pour que la « régulation » entre pleinement dans le vocabulaire juridique français, sous l'influence des États-Unis. Les États-Unis développent des autorités dites « de régulation » depuis la fin du XIX^e siècle, indépendantes du gouvernement fédéral et chargées d'encadrer des secteurs d'activité. En 1978, le président américain Jimmy Carter fait voter le *Airline Deregulation Act*, qui abolit l'autorité de régulation du transport aérien civil (*Civil Aeronautics Board*) afin de promouvoir le libre accès au marché du transport aérien et la liberté des prix. La *deregulation* mise en œuvre par Jimmy Carter sera traduite en français par « déréglementation »⁴⁸⁶. Le terme *déréglementation* se diffuse très rapidement dans les sciences économiques pour désigner la politique qui consiste à ouvrir totalement un marché à la concurrence⁴⁸⁷.

En France, l'ouverture à la concurrence débute fortement dans les années 1980 avec deux événements. En premier lieu, conformément aux promesses du candidat François Mitterrand, face au phénomène des radios pirates, la loi Fillioud de 1982 met un terme au monopole de l'État sur l'exploitation des fréquences hertziennes dans le domaine audiovisuel. La loi ouvre aux personnes privées indépendantes de l'État la possibilité d'exploiter ces ondes pour y diffuser leurs émissions de radio ou de télévision. En second lieu, à partir de 1986, une vague de privatisations sera succédée par beaucoup d'autres, et annonce un retrait durable de l'État en tant qu'acteur direct du marché⁴⁸⁸. Ces ouvertures à concurrence sont accompagnées d'une promotion de la liberté d'entreprendre bien observée en droit du travail⁴⁸⁹, de sorte que la déréglementation semble désigner le mouvement juridique qui laisse aux acteurs privés le soin de définir des règles autrefois édictées par l'État (règles d'entreprise, règles du marché...).

Seulement, **cette déréglementation a été conditionnée par l'établissement d'une régulation**. Ainsi, la loi Fillioud qui a libéralisé le secteur audiovisuel a du même coup conditionné l'exploitation des ondes hertziennes par l'obtention d'une autorisation auprès d'une autorité administrative indépendante (AAI) : la Haute autorité de la communication audiovisuelle (HACA, ancêtre du CSA), chargée de veiller au respect d'un certain nombre de

486EISEMANN Pierre-Michel, « Jacques Naveau. Droit du transport aérien international », *Politique étrangère*, n° 45, 1980, p. 1045 ; BARREAU Jocelyne et MOULINE Abdelaziz, « La déréglementation américaine des télécommunications et l'Europe : les exemples français et britanniques », *Revue d'économie industrielle*, n° 39 1987, p. 170-179 ; MENTRE Paul, « Déréglementation et politique industrielle », *Le Monde*, 13 nov. 1984

487Not. BOURGUINAT Henri, *Les Vertiges de la finance internationale*, Economica, 1987 ; DE BOISSIEU Christian, « Les innovations financières en France », *Revue d'économie politique*, vol. 96, p. 585-600

488Loi n° 86-793 du 2 juillet 1986 autorisant le Gouvernement à prendre diverses mesures d'ordre économique et social. V. aussi « Le nombre de sociétés contrôlées par l'État a été divisé par 2 en 30 ans », *La Tribune*, 2 avr. 2015. Pour une liste évidemment non-exhaustive des privatisations : Saint-Gobain (1986), Paribas, TF1, Société générale (1987), Suez (1988), Renault (1990 et 1996), Elf Aquitaine (1992), BNP (1993), Compagnie générale maritime (1996) France Telecom (1997 et 2004), Air France et Crédit lyonnais (1999), Gaz de France (2005), Électricité de France (2005 et 2008), Autoroutes du Sud de la France (2002 et 2006), Autoroutes Paris-Rhin-Rhône (2004 et 2006), Société des autoroutes du Nord et de l'Est de la France (2006), Airbus (2014), Aéroports de Paris (2013), Aéroport de Toulouse-Blagnac (2014), Aéroport de Lyon-Saint-Exupéry (2016), Aéroport de Nice-Côte d'Azur (2016), Engie et Française des jeux (2019), SNCF (2020)

489BONNECHÈRE Michèle, « Les tendances à la déréglementation et leur incidence sur la théorie des sources en droit du travail », *Droit social*, n° 1, janv. 1990, p. 40-48 ; SUPIOT Alain, « Pourquoi un droit du travail ? », *Droit social*, n° 1, janv. 1990, p. 485-493

principes par le secteur d'activité audiovisuel⁴⁹⁰. De même, la vague de privatisations de 1986 et la suppression du contrôle administratif des prix conduit le législateur à instaurer le Conseil de la concurrence, première AAI dotée d'un pouvoir propre de décision et de sanction contre les pratiques anticoncurrentielles⁴⁹¹. Ou encore, en 1997, la libéralisation de l'activité de fourniture d'accès à internet et la privatisation de France Telecom s'accompagnent de l'institution d'une AAI – l'Autorité de régulation des télécommunications, devenue l'Arcep⁴⁹² –, tout comme la privatisation d'Air France en février 1999 est succédée par la création d'une autre AAI – l'Autorité de contrôle des nuisances aéroportuaires. L'État accepte d'abandonner son interventionnisme sur le marché si une AAI régule ledit marché⁴⁹³.

Les AAI deviennent l'épicentre de la réflexion sur la régulation juridique dans les années 1980. Elles ont cinq particularités : (i) elles sont indépendantes du pouvoir exécutif ; (ii) elles concentrent des compétences normatives attribuées à la fois au législateur (édicter des normes de portée générale), à l'administration (appliquer des normes juridiques) et au juge (résoudre des différends)⁴⁹⁴ ; (iii) leur champ de compétence est limité au secteur d'activité qu'elles encadrent (tandis que la compétence du législateur, de l'administration et du juge s'étendent à la population et au territoire français) ; (iv) elles ont pour mission de concilier des principes, droits et intérêts en présence ; (v) à cette dernière fin, elles peuvent énoncer des normes juridiques non-contraignantes (avis, recommandations, lignes directrices, codes de bonnes pratiques, calendriers prévisionnels...). En examinant le phénomène des AAI – débuté en 1978 avec la création de la CNIL et de la CADA –, les juristes en droit public et en droit international semblent avoir été les premiers à importer en France le concept de régulation juridique⁴⁹⁵.

490Précisément, la HACA était chargée de veiller « *au respect du pluralisme et de l'équilibre dans les programmes* », « *au respect de la personne humaine et de la dignité, de l'égalité entre les femmes et les hommes et de la protection des enfants et des adolescents* », « *à la défense et à l'illustration de la langue française* », « *à la promotion des langues et cultures spéciales* » et « *à l'adaptation des conditions de diffusion des programmes de télévision aux difficultés particulières des sourds et des malentendants* » : loi n° 82-652 du 29 juil. 1982 sur la communication audiovisuelle, art. 14

491Ordonnance n° 86-1243 du 1^{er} décembre 1986 relative à la liberté des prix et de la concurrence, art. 2s.

492Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications (instaurant l'Autorité de régulation des télécommunications) ; et Loi n° 96-660 du 26 juillet 1996 relative à l'entreprise nationale France Télécom (privatisant partiellement France Telecom)

493COHEN-TANUGI Laurent, « L'Etat et la déréglementation : les enjeux institutionnels de la déréglementation », *Réseaux*, n° 40, 1990, p. 28 : « *En découvrant la concurrence, le marché, l'entreprise au cours des années 80, la France découvre du même coup le besoin de la régulation, car il n'est de marché efficace que correctement régulé* »

⁴⁹⁴ *Ibid.*, p. 27

495TEITGEN-COLLY Catherine, « Les autorités administratives indépendantes, histoire d'une institution », in COLLIARD Claude-Albert et TIMSIT Gérard, *Les autorités administratives indépendantes*, PUF, 1988, p. 23-24 : « *l'idée d'œuvre à réaliser tient pour les autorités administratives indépendantes à la fonction de régulation sociale qui leur est impartie dans des secteurs donnés, fonction acceptée par le groupe social considéré* ». V. aussi ROUBAN Luc, « Évaluation des politiques publiques et mouvement de dérégulation aux États-Unis », *Revue française d'administration publique*, n° 29, 1984, p. 85s. ; DELIVET Jean-Pierre et RONY Hervé, « La Commission Nationale de la Communication et des Libertés et la régulation de la communication audiovisuelle », *Revue française d'administration publique*, 1987, n° 44, p. 127-139 ; CHEVALLIER Jacques, « Les autorités administratives indépendantes : un produit d'importation ? », in BOTTINI Fabien (dir.), *Néolibéralisme et américanisation du droit*, Mare et Martin, 2019, p. 141-154

Le débat sur la régulation dépasse rapidement la thématique des AAI. Dans les années 1990, la doctrine fait le lien entre la régulation et les règles de droit souple (*soft law*), c'est-à-dire les règles de droit non contraignantes⁴⁹⁶. Certes, on vient de voir que les AAI produisent du droit souple, mais elles ne sont pas les seules : depuis la fin de la seconde guerre mondiale, le droit international est un gisement important de règles souples⁴⁹⁷ ; depuis la fin des années 1970-début des années 1980, les entreprises démultiplient les codes de bonne conduite et de déontologie⁴⁹⁸ ; et, depuis les années 1990-2000, les administrations adoptent à leur tour diverses chartes⁴⁹⁹. Le droit souple est conçu comme un moyen d'orienter les comportements en suscitant l'adhésion (*i.e.* une incitation assortie d'une bonne raison d'agir ou de ne pas agir), tandis que le droit rigide est au contraire envisagé comme un moyen d'orienter les comportements en créant de la contrainte (*i.e.* une obligation assortie d'une sanction)⁵⁰⁰.

Le mouvement d'assouplissement du droit, qui s'est accéléré depuis les années 1980, a été rapproché d'un autre mouvement apparu à la même période : l'utilisation régulière du contrat par l'administration. Comme le droit souple, le contrat offre une certaine flexibilité par la négociation, facilite l'adaptation de la règle à la volonté de ses destinataires et/ou aux intérêts en présence. Depuis 1973, dans le but d'offrir un cadre de vie agréable aux classes moyennes, l'État ouvre régulièrement un dispositif « contrats de villes moyennes », par lequel l'État apporte aux villes de taille moyenne volontaires une aide financière pour le développement, la modernisation et l'embellissement des villes cocontractantes⁵⁰¹. La contractualisation de

496« *La régulation est un processus d'ajustement des intérêts, de solution des conflits dans une société donnée. La régulation étatique ne comporte pas nécessairement la contrainte. P. Amselek (...) a souligné que sur toile de fond libérale d'un remise en cause des interventions autoritaires de l'État, les pouvoirs publics utilisent de plus en plus la direction souple des conduites* » (BONNECHÈRE Michèle, « Les tendances à la déréglementation et leur incidence sur la théorie des sources en droit du travail », *Droit social*, n° 1, janv. 1990, p. 40-48) ; le droit souple est un « *instrument de régulation sociale* » (OSMAN Filali, « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : réflexion sur la dégradation des sources privées du droit », *Revue trimestrielle de droit civil*, n° 3, 1995, p. 509-532) ; « *dans un monde en mutation et qui est à la recherche de nouveaux équilibres, l'adhésion volontaire et la persuasion nous paraissent être des méthodes de régulation sociale plus efficaces que la contrainte* » (SPYROPOULOS Georges, « Encadrement social de la mondialisation de l'économie : bilan et perspectives d'avenir de l'action normative au niveau international dans le domaine du travail », *Droit social*, n° 6, 1996, p. 551-561)

497Accroissement du nombre de *gentlemen's agreements* entre les États, apparition de standards internationaux comme les normes ISO, encadrement du droit international par des comités onusiens au moyen de recommandations, de rapports, d'observations générales, d'auditions et de constatations de violations du droit international...

498FARJAT Gérard, « Réflexions sur les codes de conduite privés », in *Mélanges B. Goldman*, Litec, 1982, p. 47 ; LAVERGNE Benjamin, *Recherche sur la soft law en droit public français*, Thèse en droit public, Toulouse, PUF, 2013, p. 63s

499Chartes du patient hospitalisé (1996), du contribuable vérifié (2001), de lutte contre le bruit (2003), du fonctionnement des EPCI... V. LAVERGNE B., *Recherche sur la soft law en droit public français*, préc., p. 60s.

500Le Conseil d'État définit ainsi le droit souple comme les « *instruments (...) [qui] ont pour objet de modifier ou d'orienter les comportements de leur destinataires en suscitant (...) leur adhésion* », qui ne sont pas créateurs « *par eux-mêmes de droits ou d'obligations pour leurs destinataires* » et qui « *présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit* » (Conseil d'État, *Le droit souple*, 2013, p. 61)

⁵⁰¹ Sénat, « L'exception territoriale : un atout pour la France », Rapport d'information n° 241, 3 avr. 2003, p. 87s.

l'action publique se généralise dans les années 1980⁵⁰², en grande partie sous l'effet des lois de 1982-1985 sur la décentralisation. En effet, ces lois transfèrent aux collectivités locales (communes, départements et régions) de nombreuses compétences autrefois dévolues à l'État (établissements scolaires préélémentaires, primaires et secondaires, transports scolaires, vaccination, aides sociales à l'enfance, aux familles et aux personnes âgées, prestations sociales, organisation des activités sportives et culturelles, ports maritimes de commerce et de pêche...). Ces transferts de compétences obligent les collectivités à coopérer étroitement avec des opérateurs économiques pour pouvoir assumer les services publics dont elles ont désormais la gestion (délégations de service public, contrats de marchés publics, contrats de partenariats...), mais aussi avec d'autres collectivités dans les domaines où leurs compétences s'enchevêtrent pour réaliser des financements croisés ou conjoints (personnes âgées, handicapés, RSA, logement social...); « *c'est pourquoi, le conventionnement ou la contractualisation deviennent des modes courants des relations administratives* »⁵⁰³. Dans les années 1990, la doctrine relie la régulation et la contractualisation de l'action publique⁵⁰⁴.

Les bouleversements juridiques des années 1980 conduisent donc les juristes à identifier les AAI, le droit souple, les conventions et contrats administratifs comme des instruments de régulation juridique. Ces instruments ont un point commun : ils contrôlent les échanges entre les êtres humains pour que le système constitué par ces êtres humains atteigne un point d'équilibre entre des phénomènes contraires (principes/droits/intérêts en présence). Lorsque la « régulation juridique » devient un concept autonome dans les années 1990-2000, elle est ainsi examinée comme la contribution des normes juridiques pour maintenir ou rétablir des équilibres dans les « *phénomènes d'interactions multiples entre social, institutions et acteurs dans le processus de production et de gestion des normes* »⁵⁰⁵, comme « *des ajustements qui permettent à la société de garder ses équilibres* »⁵⁰⁶, qu'il s'agisse dans le droit de la santé publique d'un

502 HUBRECHT Hubert-Gérald, *Les contrats de service public*, thèse Bordeaux 1980 ; AUBY Jean-François, *Les services publics locaux*, PUF, Que sais-je ?, 1982

503 BERNARD Paul, « Les relations contractuelles entre collectivités publiques : les affaires mixtes ou l'œuvre commune », *AJDA*, n° 3, 1990, p. 131s.

504 « *La régulation étatique passe par l'élaboration de politiques sectorielles, reflet des transactions passées et des compromis négociés entre les bureaucraties publiques et les intérêts sociaux qu'elles contrôlent* » (CHEVALLIER Jacques, « Décentralisation et politiques publiques », *AJDA*, avr. 1992, p. 120-127) ; « *pour mettre en œuvre sa nouvelle politique urbaine, l'État utilise un autre procédé classique de régulation : le contrat* » (JÉGOUZO Yves, « La décentralisation et la ville », *AJDA*, avr. 1992, p. 108-109)

505 COMMAILLE Jacques, « Normes juridiques et régulation sociale. Retour à la sociologie générale » in CHAZEL François et COMMAILLE J. (dir.), *Normes juridiques et régulation sociale*, Journées d'études 1987, Bordeaux, LGDJ, 1991, p. 21 : « *En fait, le fonctionnement et la reproduction des systèmes sociaux complexes s'établissent suivant une régulation sociale, dont la régulation juridique participe, constituée d'équilibres maintenus ou retrouvés, mais aussi de tensions, de ruptures, e contradictions provoquées par la multiplicité des instances et des acteurs sociaux impliqués ainsi que par la pluralité des stratégies sociales à l'œuvre* » (p. 21)

506 MAISL Herbert, « La régulation des télécommunications, changements et perspectives », *RFDA*, mai 1995, p. 449s. : « *la réglementation peut se définir comme l'encadrement juridique des comportements sociaux (...). Mais le terme de régulation a un sens plus large : on parle de régulation du trafic sur le réseau routier ou, plus généralement, de régulation d'un système pour désigner l'action visant à réguler le mouvement, à assurer son bon fonctionnement, à maintenir son équilibre. La réglementation est ainsi un mode de régulation parmi l'ensemble des ajustements (...) qui permettent à la société de garder ses équilibres. Lorsque les juristes parlent de régulation, ils admettent que les méthodes de réglementation traditionnelles sont en crise et qu'une re-*

équilibre besoin de santé de la population / coûts du système de soins⁵⁰⁷ ou encore, dans le droit de la concurrence, d'un équilibre libre concurrence / autres droits, intérêts et principes protégés juridiquement⁵⁰⁸. En s'appuyant sur le contrôle des échanges que les composants d'un système entretiennent entre eux et avec le milieu extérieur pour orienter ce système vers un point d'équilibre, la régulation juridique acquiert une signification qui s'aligne sur la définition transdisciplinaire de la régulation qu'on a proposée. En ce sens, Marie-Anne Frison-Roche définit la régulation comme « *l'ensemble des instruments corrélés entre eux ayant vocation à engendrer et à maintenir des équilibres là où les seules forces en présence ne les produisent pas* »⁵⁰⁹.

2. La France des années 2020, submergée par la régulation juridique

Ces observations nous amènent à définir la **régulation juridique** comme le **procédé consistant à créer des normes juridiques ou à utiliser des normes juridiques existantes pour contrôler les échanges que les composants du système régulé** (institution, secteur d'activité, ordre juridique...) **entretiennent entre eux et avec le milieu extérieur, de façon à orienter ce système vers un point d'équilibre où se compensent des effets contraires traversant ce système** (besoins de santé / coûts du système de santé, libre concurrence / préservation de l'environnement naturel etc.). On a vu que des institutions (p. ex. les performances d'une administration) et des secteurs d'activité (p. ex. le secteur audiovisuel) sont des systèmes régulables juridiquement, mais il en est de même pour les ordres juridiques. On appelle « ordre juridique » l'ensemble des normes juridiques qui entretiennent des rapports hiérarchiques les unes avec les autres⁵¹⁰. L'analyse de Kelsen propose un encadrement de l'ordre juridique *par hiérarchisation* et non *par régulation*, donc cette analyse ne cherche pas à orienter l'ordre juridique vers un point d'équilibre pour résoudre les problèmes de conflits de normes qui perturbent cet ordre.

Pour autant, l'ordre juridique est de plus en plus *régulé* depuis les années 1930, surtout depuis les années 1970-1980. On a vu que l'accroissement du nombre de droits et libertés depuis la fin du XIXe siècle et que la normativité reconnue à la Constitution et au droit international après la seconde guerre mondiale ont favorisé les risques et occasions de conflits entre des droits, principes et intérêts contraires. Il a donc fallu à l'État trouver un point d'équilibre où se

réglementation doit se définir : notamment, pour assurer les équilibres du marché et la défense de l'intérêt général, en étant parfois plus incitatif que normatif et plus dissuasif que répressif »

507DELAHAYE-GUILLOCHEAU Valérie et METTENDORFF Martial, *Droit social*, sept. 1997, p. 859-865 : « *La régulation du système hospitalier ne [consiste] pas en la seule maîtrise des dépenses d'assurance-maladie, mais plus fondamentalement en la combinaison d'instruments multiples permettant la production par l'ensemble du système d'une réponse optimale aux besoins de la population en matière de soins hospitaliers au meilleur coût pour la collectivité* »

508FRISON-ROCHE M.-A., « Le droit de la régulation », *Recueil Dalloz*, fév. 2001, p. 610-617

509 FRISON-ROCHE M.-A., « Le droit, source et forme de régulation mondiale », in JACQUET Pierre, PISANI-FERRY Jean et TUBIANA Laurence (dir.), *Gouvernance mondiale*, La Documentation française, 2002, p. 314

510 Par exemple, la loi française entretient des rapports hiérarchiques avec la constitution françaises, donc la loi et la constitution françaises intègrent le même ordre juridique. Au contraire, la loi indienne n'entretient pas de rapports hiérarchiques avec la loi ou la constitution françaises, donc la loi indienne n'intègre pas le même ordre juridique que la loi et la constitution françaises. En revanche, si l'administration, le juge ou le législateur français reconnaît une valeur juridique à une loi indienne de telle manière que cette dernière gagne une place dans la hiérarchie française des normes juridiques, alors cette loi indienne intègre l'ordre juridique français.

compensent les droits et principes contraires, un point d'équilibre où ces droits et principes peuvent se concilier suffisamment pour que l'un ne prive pas l'autre de toute réalité concrète, de tout effet utile.

Dès 1933, dans une affaire où un arrêté municipal interdisait l'organisation dans la commune de deux conférences faisant intervenir l'écrivain d'extrême droite René Benjamin, le juge administratif est appelé à concilier liberté de réunion et sauvegarde de l'ordre public⁵¹¹. À cette occasion, le Conseil d'État exige qu'une mesure restreignant un droit ou une liberté soit adaptée au « *degré de gravité* » de la menace pour l'ordre public. Depuis les années 1970, le Conseil d'État conditionne la validité d'un projet d'utilité publique (i.e. un projet d'urbanisme impliquant une expropriation) par une mise en balance des avantages et inconvénients du projet – coût, impact environnemental, impact sur la propriété privée...⁵¹² –, et se reconnaît compétent pour contrôler les erreurs *manifestes* commises par l'administration lorsqu'elle apprécie la sauvegarde de l'ordre public⁵¹³. La doctrine interprète cette théorie du bilan et ce contrôle de l'erreur manifeste d'appréciation comme des consécration d'un « contrôle de proportionnalité » par lequel le juge administratif vérifie l'absence de disproportion des mesures administratives (« *par excessivité ou par pusillanimité* » pour reprendre la formule de Michel Guibal)⁵¹⁴. En s'inspirant de la doctrine⁵¹⁵ et de la loi Auroux de 1982⁵¹⁶, le Conseil d'État

⁵¹¹ CE, *Benjamin*, 19 mai 1933, n° 17413

⁵¹²« Théorie du bilan » consacrée par CE, Ass., *Ville Nouvelle-Est*, 28 mai 1971, n° 78825 : « *une opération ne peut être légalement déclarée d'utilité publique [et donc engendrer une expropriation] que si les atteintes à la propriété privée, le coût financier et éventuellement les inconvénients d'ordre social qu'elle comporte ne sont pas excessifs eu égard à l'intérêt qu'elle présente* »

⁵¹³« Contrôle de l'erreur manifeste d'appréciation » consacré par CE, Ass., *Librairie François Maspero*, 2 nov. 1973, n° 82590

⁵¹⁴BRAIBANT Guy, « Le principe de proportionnalité », in *Mélanges offerts à Marcel Waline. Le juge et le droit public.*, LGDJ, Tome 2, 1974, p. 297-306 ; dans le même ouvrage, v. LEMASURIER Jeanne, « Vers un Nouveau Principe Général du Droit ? Le Principe "Bilan-Coût-Avantages" », p. 551-562 ; GUIBAL Michel, « De la proportionnalité », *AJDA*, 1978, p. 477s.

⁵¹⁵PHILIPPE Xavier, *Le contrôle de proportionnalité dans les jurisprudences constitutionnelle et administrative françaises*, Economica; 1990, 542 p.

⁵¹⁶La loi Auroux modifie le Code du travail pour y prévoir que le règlement intérieur d'une entreprise « *ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ». À partir de 1987, le Conseil d'État est régulièrement saisi sur cette disposition par le personnel administratif non titularisé, donc soumis à un contrat de travail et au Code du travail. Cela conduit la juridiction administrative suprême à vérifier que le règlement intérieur d'une entreprise ne porte pas une atteinte disproportionnée aux droits et libertés de ces travailleurs. Par exemple, la disposition du règlement intérieur stipulant que « *la direction se réserve le droit de faire ouvrir à tout moment (...) afin d'en contrôler le contenu* » les vestiaires ou armoires individuelles des salariés « *excède l'étendue des restrictions que l'employeur peut légalement apporter aux droits des personnes et aux libertés individuelles en vue d'assurer l'hygiène et la sécurité dans l'entreprise* » ; inversement, un règlement intérieur qui prévoit le contrôle des membres du personnel avec des détecteurs de métaux porte certes atteinte aux droits des personnes, mais « *une telle atteinte doit être regardée, en l'espèce, comme justifiée par les nécessités spécifiques de la prévention des vols et proportionnée à ce but, sans que le consentement des salariés soit requis et même en l'absence de circonstances exceptionnelles ou de présomptions graves* » (CE, Sect., *Société Gantois*, 12 juin 1987, n° 72388 et CE, Sous-sect. réunies, *Comptoir Lyon Alemand Louyot*, 8 juil. 1988)

consacre explicitement son contrôle de proportionnalité en 1988⁵¹⁷. Le contrôle de proportionnalité pratiqué par le Conseil d'État consiste à vérifier qu'une mesure administrative est proportionnée au but de la mesure et, de façon moins importante, à la gravité des faits. Il peut ainsi être défini comme « *l'exigence d'un rapport, d'une adéquation et d'un équilibre entre les moyens employés par l'Administration (...), le but qu'elle vise (...) [et] la situation de fait dans laquelle s'applique la décision administrative. (...) Il doit s'établir un rapport de juste proportion entre la situation, la finalité et la décision* »⁵¹⁸.

Le contrôle de proportionnalité aboutit à écarter l'application d'une norme – la norme disproportionnée (p. ex. arrêté municipal interdisant des conférences) ou, si cette dernière est proportionnée, la norme concurrente (p. ex. liberté de réunion). Cet outil, qui conduit à écarter une norme dans un cas d'espèce (contrôle *in concreto*) ou dans tous les cas d'espèce (contrôle *in abstracto*), est donc d'un grand secours pour résoudre des conflits entre des normes d'égale valeur juridique, c'est-à-dire occupant la même place dans la hiérarchie des normes. En somme, le contrôle de proportionnalité est une technique régulatrice de l'ordre juridique qui consiste à contrôler les échanges entre les normes de même valeur juridique, de façon à orienter cet ordre vers des points d'équilibre où sont éliminées les perturbations provoquées par les conflits de normes. Le Conseil constitutionnel intègre le contrôle de proportionnalité *in abstracto* dans sa jurisprudence au cours des années 1990, d'abord pour s'assurer que le législateur adopte des lois en respectant le but assigné à la loi de servir l'intérêt général et non des volontés partisans⁵¹⁹, ensuite pour résoudre les conflits entre des principes et/ou des droits ayant tous une valeur constitutionnelle⁵²⁰. Quant à la Cour de cassation, depuis les années 1980 et après avoir reconnu la valeur juridique des conventions internationales, elle applique le contrôle de

517CE, Sect., *Sté Bernard X.*, 27 avr. 1988, n° 63772. En l'espèce, le gouvernement avait adopté un arrêté qui suspendait, durant un an, la fabrication, l'exportation, l'importation et la mise sur le marché de gommes à effacer, au motif que ces gommes peuvent rappeler des denrées alimentaires et être facilement ingérées par les enfants. Le Conseil d'État estime que le gouvernement n'a « *pas adopté une mesure excessive et disproportionnée au regard des risques pour la santé des jeunes enfants que présentaient les objets en cause* ».

518ÇALISKAN Ziya A., « Le juge administratif français et le principe de proportionnalité », *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, n° 12, 2004

519À ce titre, le Conseil constitutionnel vérifie que « *les modalités retenues par la loi ne sont pas manifestement inappropriées à l'objectif poursuivi* » (CC, Décision n° 90-280 DC du 6 décembre 1990, *Loi organisant la concomitance des renouvellements des conseils généraux et des conseils régionaux*, cons. 26). V. aussi GOESEL-LE BIHAN Valérie, « Le juge constitutionnel et la proportionnalité », *Annuaire international de justice constitutionnelle*, n° 25, 2010, p. 191-212

520CC, Décision n° 93-323 DC du 5 août 1993, *Loi relative aux contrôles et vérifications d'identité*, cons. 15, où le Conseil constitutionnel vérifie pour la première fois que le législateur garantit « *l'équilibre que la Constitution impose d'assurer entre les nécessités d'ordre public et la sauvegarde de la liberté individuelle* ». GOESEL-LE BIHAN V., « Le contrôle de proportionnalité exercé par le Conseil constitutionnel », *Cahiers du Conseil constitutionnel*, n° 22, juin 2007 : « *si le contrôle de proportionnalité impose la recherche d'un équilibre entre les atteintes portées aux droits et libertés constitutionnels et les objectifs poursuivis, l'étendue du contrôle exercé est en elle-même le résultat d'un équilibre entre exigences logiques, au sacrifice desquelles le juge ne peut se résoudre au-delà d'un certain seuil, et respect des compétences attribuées à l'organe contrôlé* »

proportionnalité *in concreto* dans de nombreux litiges où sont invoqués des droits d'égalité de valeur et/ou tirés de la Convention EDH⁵²¹.

Pour conclure, il est aujourd'hui communément admis que la régulation juridique a pour fonction « *la réalisation d'un équilibre (...) qui implique la conciliation d'intérêts contradictoires* »⁵²² – on dira quant à nous « la réalisation d'un équilibre qui implique la compensation d'effets contraires ». Pour atteindre un point d'équilibre, il peut être nécessaire d'obtenir l'adhésion (droit souple) comme il peut être nécessaire de contraindre (droit rigide), de sorte que le droit souple et le droit rigide sont tous deux des moyens de la régulation juridique. Surtout, dès lors qu'un système atteint un point d'équilibre grâce aux échanges de ses composants entre eux et avec le milieu extérieur, la régulation juridique tente de contrôler ces échanges. En ce sens, les deux premiers systèmes régulés par l'État en France ont probablement été le budget et la monnaie. Si on considère que l'État en France est apparu entre les mérovingiens et les carolingiens (VIe-VIIIe siècle), on peut estimer que l'État a commencé par réguler le budget dès les VIe-VIIIe siècles en recherchant des sources de revenus pour équilibrer les dépenses et les recettes des finances publiques⁵²³. Quant à la monnaie, les mérovingiens ont tenté d'équilibrer sa valeur à partir de la fin du VIe siècle⁵²⁴ mais ce sont surtout les carolingiens qui, depuis la deuxième moitié du VIIIe siècle, instrumentalisent la valeur de la monnaie pour corriger des déséquilibres économiques ou budgétaires à coups de réévaluations et

521P. ex. C. Cass., 1^{re} Civ., 31 janv. 1989, n° 87-15.139 (qui, lorsque s'opposent la liberté d'expression issue de la Convention EDH et la protection de la réputation d'autrui, exige au juge du fond de vérifier que la mesure restreignant la liberté d'expression est en « *adéquation (...) [avec] le but poursuivi* ») ; C. Cass., 1^{re} Civ., 29 oct. 1990, n° 88-19.366 (qui exige au juge du fond de rechercher le « *nécessaire équilibre* » entre les droits d'égalité de valeur à la liberté d'expression et de pratiquer sa religion)

522OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse de droit, HAL, 2014, p. 291s.

523Vers les VIe-VIIe siècles, on constate l'existence dans le Royaume des Francs de contributions publiques non féodales, qui conduisent l'historien Shoichi Sato à y voir la base fiscale constitutive d'un État (SATO Shoichi, « À propos de la fiscalité et de l'État mérovingien aux VIe et VIIe siècles » in CAROZZI Claude et TAVIANI-CAROZZI Huguette (dir.), *Le médiéviste devant ses sources*, PUF de Provence, 2004, p. 171-183). Surtout, aux débuts de l'époque carolingienne (VIIIe-IXe siècles), il est désormais acquis que le Royaume des francs, en plus de reposer sur une administration de dizaines de milliers de fonctionnaires, possédait les quatre caractéristiques reconnues à un État par des historiens – le *regnum* (exercice de l'autorité souveraine sur un territoire délimité), l'*ecclesia* (homogénéité culturelle), l'*imperium* (monopole organisé de la violence légitime) et la *res publica* (pouvoir suprême qui dépasse la personne du Roi) : v. DURLIAT Jean, *Les finances publiques de Dioclétien aux Carolingiens (284-889)*, Sigmaringen, Thorbecke, 1990, p. 230s. ; et GRUNIN Andrey, « "Imaginer l'Empire". Étude d'un concept étatique carolingien et évolution du vocabulaire politique dans le royaume et l'empire franc (768-840) et dans la *Francia Occidentalis* (840-877) », *Revue de l'IFHA*, n° 3, 2011

524Ces réformes avaient pour objectif d'uniformiser la valeur des monnaies entre les royaumes d'Austrasie et de Burgondie après la signature du traité d'Andelot de 587 qui prévoyait la libre circulation des personnes et des biens entre ces royaumes. Ainsi, vers 587, les mérovingiens instaurent des monnaies nationales en standardisant leur aspect, en généralisant le tremissis (monnaie romaine) pour remplacer la principale monnaie concurrente (le solidus) et en réduisant leur poids de 24 siliques (4,53g) à 21 siliques (3,94g). Vers 670, les mérovingiens établissent le denier qui remplacera progressivement le tremissis, mais le droit de frappe est si dispersé que l'État n'a aucun contrôle sur la création de monnaie. V. LAUWERS Christian, « Les pouvoirs émetteurs mérovingiens », *Bulletin de la Société tournaisienne de géologie, Préhistoire et archéologie*, Vol. XIV, n° 7, sept. 2016, p. 198-209

dévaluations⁵²⁵. Outre le budget et la monnaie, l'État régule aussi le marché économique de longue date. Au Moyen-Âge, les politiques économiques dépendaient des lois économiques identifiées (telle circonstance provoque mécaniquement telle conséquence) mais ne dépendaient pas encore d'équilibres économiques (compensation de lois économiques contraires)⁵²⁶. C'est dans les années 1920 que les théories économiques néoclassiques pénètrent les débats parlementaires et influencent les décisions du législateur⁵²⁷. Toutefois, la régulation juridique des conduites humaines est un phénomène plus nouveau. Jusqu'à la deuxième moitié du XXe siècle, les conduites humaines ont été juridiquement encadrées dans l'espoir que la contrainte suffirait à éliminer les comportements néfastes. Depuis les années 1970-1980, les conduites humaines sont de plus en plus encadrées par le contrôle des échanges entre les êtres humains ou entre les normes pour orienter leur système d'appartenance (secteur d'activité, ordre juridique, institution...) vers un point d'équilibre.

À l'heure où on rédige ces lignes en 2023, une part considérable de l'encadrement juridique relève de la régulation : les **atteintes portées aux droits et libertés par des mesures de préservation de l'ordre public ou de l'intérêt général** doivent respecter un certain équilibre vérifié par le juge entre les moyens déployés par la mesure / but de la mesure / gravité des faits

525 Entre 754 et 765, Pépin le Bref centralise le droit de frappe et limite le poids minimal du denier à 1,27g, et Charlemagne relève ce seuil à 1,36g en 777 puis à 2g en 781, mais ces réévaluations successives de la monnaie seront suivies d'une politique de dévaluation de la monnaie au IXe siècle : DOHEAERD Renée, « Les reformes monétaires carolingiennes », *Annales. Economies, sociétés, civilisations*, 7^e année, n° 1, 1952, p.13-20

526 L'école scolastique du XIe siècle prônait la fixation d'un prix juste (moralement) ; l'école mercantiliste du XVIe siècle identifie des lois économiques systématiques sur lesquelles les marchands (Pierre de Boisguilbert) et l'État (Thomas Mun, Jean Bodin) peuvent s'appuyer pour augmenter leurs richesses (Jean Bodin était un célèbre mercantiliste) ; et l'école physiocrate du XVIIIe siècle s'appuie à son tour sur une loi économique fondamentale qui met en relation la hausse du capital (avances par les propriétaires fonciers) avec le profit (produit net obtenu par les propriétaires). Mais aucune de ces écoles ne réfléchit l'économie en termes d'équilibres, jusqu'à la naissance de l'école néo-classique portée par Léon Walras à la fin du XIXe siècle.

527 « Il n'y aurait rien de choquant (...) à laisser aux ateliers de la marine, actuellement spécialisés, le soin d'exercer une sorte de régulation des prix » (Chambre des députés, Intervention du député de Paris Louis Jaurès, 1^e séance du 11 juin 1926, JO de 1926, p. 2487-2488) ; « La crise que nous subissons actuellement (...) est une crise de déséquilibres dans la déflation économique et dans la baisse des prix, qui succède à une crise de déséquilibre dans l'inflation monétaire et dans la hausse des prix. (...) Vous avez préféré (...) la méthode de paresse, qui tendait à laisser la vie économique suivre son cours, à laisser la crise se développer d'elle-même et le rajustement se faire tout seul, par le jeu spontané (...) de la vie économique » (Chambre des députés, Intervention du député Étienne Antonelli, séance du 11 fév. 1927, JO 1927, p. 365) ; « Il ne serait peut-être pas inutile d'envisager une disposition prévoyant que l'État garantira le cultivateur contre le risque de perte, que le cultivateur qui aura accepté l'opération sera toujours assuré de pouvoir retrouver (...) le capital qu'il aura entreposé et conservé. (...) Nous espérons (...) que bientôt vous [s'adresse au ministre de l'agriculture] reviendrez ici avec des projets organiques, de nature à donner au marché cette stabilité et cette régulation qui lui ont manqué jusqu'à présent » (Chambre des députés, Intervention de Pierre Mendès-France, 2^e séance du 27 déc. 1932, JO de 1932, p. 3707) ; « ces [crédits] ne seront pas (...) un élément de perturbation et de désordre. (...) Ils peuvent être un élément de régulation et d'équilibre pour le marché » (Chambre des députés, Intervention de Georges Potut invitant le gouvernement à promouvoir une politique de crédits pour combler le déficit, 2^e séance du 25 janv. 1935, JO de 1935, p. 222)

auxquels s'applique la mesure⁵²⁸ ; les **projets d'utilité publique** sont eux aussi soumis à un équilibre vérifié par le juge avantages du projet / inconvénients du projet sur l'économie, l'environnement, la société et la propriété privée ; les **traitements de données à caractère personnel** dépendent d'un équilibre vérifié par la CNIL entre le principe de finalité / pertinence des données collectées / durée de conservation des données / sécurité et confidentialité des données conservées / droits des personnes / intérêt légitime du responsable de traitement de données ; le **système de santé publique** doit obéir à un certain équilibre besoins de santé / coûts du système de santé ; le **divorce par consentement mutuel** est soumis à un équilibre recherché par les parties, le cas échéant dans le cadre d'une médiation prescrite par le juge⁵²⁹ ; les **contrats de consommation et entre professionnels** ne doivent pas contenir de clause qui provoquerait un déséquilibre significatif entre les obligations des cocontractants⁵³⁰ ; la décision prise par le médecin d'**arrêter le traitement, l'alimentation et l'hydratation artificielles d'un patient en fin de vie** (euthanasie passive) n'est légale que si elle observe un équilibre vérifié par le juge

⁵²⁸ À l'exception des droits indérogeables (à ne pas subir de torture ni de traitement dégradant et inhumain, à ne pas être réduit en esclavage ou en servitude, et à ne pas se voir appliqué rétroactivement une sanction pénale plus lourde), tous les droits, toutes les libertés, tous les principes d'égale valeur sont soumis à la recherche d'un équilibre en cas de conflit – qu'il s'agisse de la liberté de réunion (CE, *Benjamin*, 1933) du droit au respect de la vie privée (CE, Ass., *M. Belgacem*, 19 avr. 1991, n° 107470), de la liberté de circulation (CE, *M. Chaline Le Garrec*, 2 oct. 1991, n° 65758 ; CE Sect., *M. Doumenjoud*, 11 déc. 2015, n° 395009), de la liberté d'expression (CE, Sect., *Association Gurekin et Coordination des comités de soutien aux prisonniers politiques basques*, 30 juil. 2003, n° 237649), de la dignité humaine (CE, ord. ref., *Dieudonné*, 9 janv. 2014, n° 374508)... Ainsi le Conseil constitutionnel a-t-il évalué la conformité des lois à la Constitution selon des équilibres dignité de la personne humaine / liberté de la femme qui découle de l'art. 2 de la Déclaration de 1789 (CC, Décision n° 2001-446 DC du 27 juin 2001, *Loi relative à l'interruption volontaire de grossesse et à la contraception*, cons. 5), droit au respect de la vie privée / sauvegarde de l'ordre public (CC, décision n° 2009-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, cons. 27), liberté d'entreprendre et liberté contractuelle / principe d'intérêt général du pluralisme des courants d'expression (CC, décision n° 2005-497 DC du 1^{er} juil. 2004, *Loi relative aux communications électroniques et aux services de communication audiovisuelle*, cons. 20), prévention des atteintes à l'ordre public / présomption d'innocence et autres droits de la défense (CC, décision n° 2010-14 QPC du 30 juil. 2010, *M. Daniel W. et autres [Garde à vue]*, cons. 29)...

⁵²⁹ En droit la famille, l'art. 5 de la loi n° 2002-305 du 4 mars 2002 relative à l'autorité parentale instaure une égalité entre les deux parents (coparentalité) : après la séparation, l'enfant maintient en principe les liens avec les deux parents, la résidence alternée est légalisée, et les décisions importantes concernant la vie de l'enfant doivent être prises d'un commun accord. L'égale responsabilité des deux parents vis-à-vis de l'enfant implique un dialogue entre les parents et donc un certain équilibre parental. Ces nouvelles bases conduisent le législateur de 2004 à favoriser le règlement amiable en cas de divorce pour obliger les parents à trouver une solution responsable et, à cette fin, autorise le juge à prononcer une mesure de médiation familiale (loi n° 2004-439 du 26 mai 2004 relative au divorce, art. 11 et 12). En 2016, le législateur supprime l'obligation de passer devant le juge aux affaires familiales pour les époux qui divorcent par consentement mutuel (Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e siècle, art. 50).

⁵³⁰ Ce déséquilibre peut être évalué par le juge, par la Commission des clauses abusives et par la DGCCRF. La notion de « déséquilibre significatif » a d'abord été introduite pour les contrats de consommation par la directive européenne 93/13/CEE du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (transposée en France par la loi n° 95-96 du 1^{er} février 1995 concernant les clauses abusives et la présentation des contrats et régissant diverses activités d'ordre économique et commercial) puis, pour les contrats entre professionnels, par la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie

entre droit au respect de la vie / droit du patient à ne pas subir d'obstination déraisonnable⁵³¹ ; la **violation d'un droit d'auteur** est évaluée par l'Arcom selon un équilibre protection des œuvres / libertés d'usage des œuvres⁵³² etc. Surtout, une quantité vertigineuse de secteurs d'activité est désormais placée sous régulation étatique : le traitement de données personnelles, qu'on a déjà cité (avec la CNIL) ; **l'accès aux documents administratifs** (CADA) ; le **secteur audiovisuel et des communications électroniques** (Arcom) ; la **concurrence économique** (Autorité de la concurrence) ; le **financement des campagnes électorales** (Commission nationale des comptes de campagne et des financements politiques) ; la **fourniture de réseaux de communications électroniques** (Arcep) ; le **secret de la défense nationale** (Commission du secret de la défense nationale) ; les **nuisances sonores aéroportuaires** (Autorité de contrôle des nuisances aéroportuaires) ; le **marché de l'énergie électrique et du gaz** (Commission de régulation de l'énergie) ; les **marchés d'instruments financiers** (Autorité des marchés financiers) ; la **sécurité nucléaire** (Autorité de sûreté nucléaire) ; les **conditions de prise en charge et de transfèrement des personnes privées de libertés** (Contrôleur général des lieux de privation de liberté) ; les **jeux d'argent et de hasard en ligne** (Autorité nationale des jeux) ; **l'évaluation de l'enseignement supérieur et de la recherche** (Haut Conseil de l'évaluation de la recherche et de l'enseignement supérieur) ; les **techniques déployées par les services de renseignement** (Commission nationale de contrôle des techniques de renseignement) etc.

B) Concepts mobilisés pour réguler juridiquement le réseau internet

On a défini la régulation d'un système comme la méthode qui consiste à neutraliser les problèmes perturbant ce système, en s'appuyant sur des règles pour contrôler les échanges qu'entretiennent les composants de ce système entre eux et avec le milieu extérieur à internet, de façon à orienter ce système vers un point d'équilibre où se compensent les effets contraires dont le déséquilibre perturbe ledit système. On a vu que la régulation *juridique* consiste à appliquer cette même méthode en s'appuyant sur des *normes juridiques* pour contrôler les échanges qu'entretiennent les composants du système entre eux et avec le milieu extérieur. Ces définitions nous permettent de préciser les contours de la régulation juridique appliquée au réseau internet.

1/ Quel est le système qu'on cherche à réguler juridiquement dans le cadre de cette thèse ? La question s'impose dès lors que toute régulation s'applique à un système. On ne cherche évidemment pas à réguler toutes les réalités qu'implique le système « internet », tant ces réalités sont nombreuses. Cette thèse est rédigée dans le but de proposer une méthode de régulation capable d'encadrer les rapports de force interhumains en ligne pour réduire efficacement l'échelle des dommages nés sur internet. On identifie quatre sources de dommage sur ce réseau. Les dommages survenant par internet proviennent soit d'une défectuosité de la machine (panne indépendante d'une cyberattaque, effacement de la mémoire par obsolescence du matériel...), soit d'une insuffisance de ressources (mémoire épuisée par le volume de données, fréquences hertziennes indisponibles pour accéder à un service en ligne...), soit d'une intervention extérieure qui dégrade les composants de la machine (détérioration voire destruction d'une machine par une personne ou une autre machine...), soit enfin de l'exécution de données stockées. On ne s'intéressera pas aux trois premières sources de dommages, mais seulement aux dommages issus de l'exécution de

⁵³¹ CE, Ass., 24 juin 2014, *Mme Lambert*, n° 375081, 375090 et 37509

⁵³² Arcom, « Garantir l'équilibre entre la protection et l'exploitation des œuvres sur les plateformes en ligne », consulté le 10 novembre 2023

données stockées (logiciel malveillant, contenu haineux, fausses informations, consommation illicite d'œuvres protégées, achats et ventes illicites, pédocriminalité en ligne...).

Il est important de comprendre ce cadre de notre étude : on ne cherche pas ici à réduire la gravité des dommages nés sur internet, mais seulement leur échelle de diffusion dans le cyberspace⁵³³. Il nous semble donc important de compléter cette étude par d'autres travaux spécialisés dans l'atténuation de la gravité des dommages nés sur internet. Par conséquent, **le système qu'on cherche à réguler ici est l'échelle de diffusion d'une donnée stockée dans le cyberspace** (*i.e.* stockée par une ou plusieurs machines connectées à internet).

2/ Quels sont les composants du système dont on cherche à contrôler les échanges ?

Pour y répondre, on peut d'abord se demander comment est alimentée l'échelle de diffusion d'une donnée dans le cyberspace. Pour exister sur une machine, une donnée doit être présente dans la mémoire de cette machine. Or, on ne connaît que deux moyens pour intégrer une donnée dans la mémoire d'une machine : soit en produisant une donnée depuis cette machine ; soit en stockant une donnée sur cette machine.

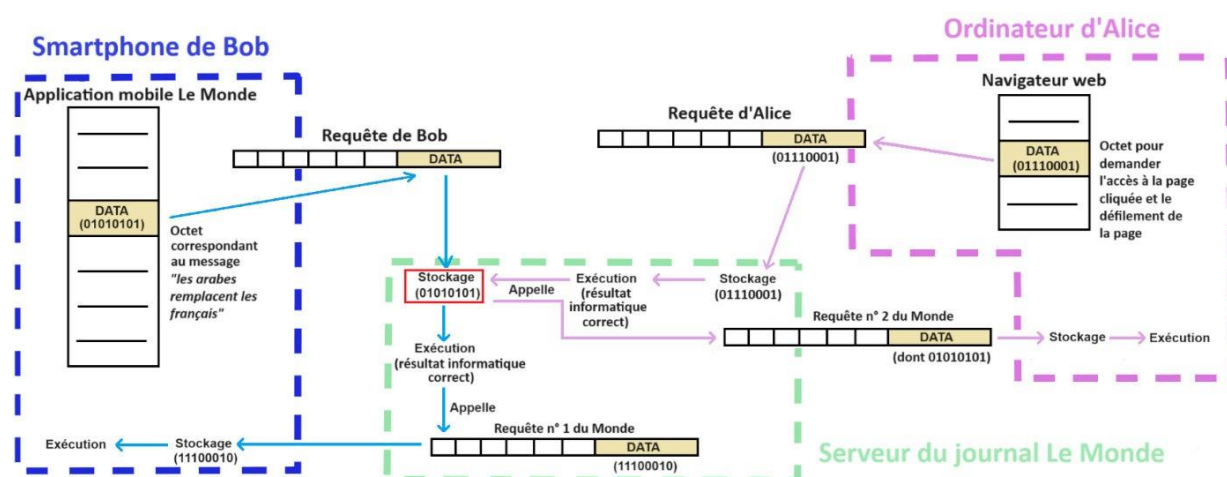
On mesure ainsi l'échelle de diffusion d'une donnée par le nombre de machine différentes qui produisent ou qui stockent cette donnée. Deux types d'échelle de diffusion seront distinguées : l'échelle de diffusion abstraite d'une donnée, c'est-à-dire le nombre de machines différentes sur lesquelles cette donnée est accessible (par exemple 1 000 machines différentes qui stockent le logiciel Acrobat d'Adobe) ; et l'échelle de diffusion concrète d'une donnée, c'est-à-dire le nombre de machines différentes qui accèdent réellement à cette donnée, qui en demandent l'exécution (par exemple 500 machines qui exécutent le logiciel Acrobat d'Adobe). Dans le cadre de cette thèse, on s'intéresse seulement à l'échelle de diffusion concrète d'une donnée. Pour simplifier la lecture, on abrègera par la suite « échelle de diffusion » l'échelle de diffusion *concrète* d'une donnée. Une machine qui stocke un logiciel qu'elle n'exécute jamais n'intégrera donc pas l'« échelle de diffusion » (concrète) de ce logiciel. En suivant ce même souci de simplification, chaque fois que sera évoquée la « production ou le stockage » d'une donnée, il sera question d'une production ou d'un stockage concret, effectué dans le cadre d'une requête d'accès (à l'exclusion donc des productions et stockages abstraits, effectués en-dehors de toute requête d'accès).

Prenons l'exemple d'un utilisateur du logiciel Word, qui rédige un texte unique, introuvable ailleurs. Dans ce cas, l'ordinateur de cet utilisateur est la seule machine qui produit les données constitutives de ce texte. C'est aussi la seule machine qui stocke ce document texte, si l'utilisateur ne l'a pas partagé avec d'autres. Par conséquent, l'échelle de diffusion des données constitutives de ce document s'élève à une seule et même machine qui produit et qui stocke ce document – l'ordinateur de l'utilisateur. *A contrario*, les données constitutives du logiciel Word lui-même sont stockées par plus d'un milliard de machines connectées à internet dans le monde, de sorte que l'échelle de diffusion de ce logiciel s'élève à plus d'un milliard de machines. Ces deux exemples désignent des échelles de diffusion dans des réseaux locaux

533Par exemple, une cyberattaque peut affecter seulement 20 machines, mais ces 20 machines ont une importance cruciale pour le fonctionnement économique, social, institutionnel, industriel, hospitalier ou environnemental d'un pays. Dans ce cas, l'échelle de diffusion est faible, mais les conséquences peuvent être bien plus graves qu'une cyberattaque affectant 10 000 machines d'utilisateurs. On se concentrera ici sur la régulation de l'échelle de diffusion, et non de la gravité des dommages.

Comment différencier la production et le stockage d'une donnée ? Comment appliquer ces concepts à l'échelle de diffusion d'une donnée dans le cyberspace, c'est-à-dire au-delà d'un réseau local ? On reprend notre exemple de l'utilisateur Bob qui, depuis l'application mobile du journal Le Monde, publie le commentaire : « *les arabes remplacent les français* » (octet 01010101). Une fois la requête de publication de Bob réceptionnée par le serveur du Monde, ce serveur stocke dans sa base de données les octets correspondant à ce message (01010101). Le serveur du Monde stocke cet octet pour pouvoir l'exécuter. Si le résultat informatique est correct à l'issue de l'exécution, c'est-à-dire s'il correspond au résultat attendu pour l'octet 01010101, alors le serveur du Monde recherche dans sa mémoire les données qui doivent être renvoyées à Bob pour lui confirmer la bonne exécution de sa requête. Dès que le serveur a trouvé les données pertinentes dans sa mémoire, il formule donc une requête destinée au smartphone de Bob et comportant les octets confirmant la bonne exécution de son message (11100010). Le smartphone de Bob n'a plus qu'à réceptionner la requête envoyée par le serveur du Monde, puis à exécuter ladite requête. À l'issue de cette exécution, Bob verra alors s'afficher sur son smartphone le message qu'il vient de publier sur les serveurs du Monde.

Ajoutons à présent l'utilisatrice Alice qui, depuis le navigateur web de son ordinateur, souhaite accéder à la section « commentaires » de l'article du Monde sous lequel est publié le message de Bob. Jouant le rôle de client pour Alice en l'espèce, le navigateur comporte un octet 01110001 qui correspond (fictivement ici) aux actions d'accéder à la page web cliquée et de faire défiler la page web (pour atteindre la section commentaires). L'ordinateur d'Alice émet donc une requête qui contient, dans son champ DATA, l'octet 01110001 et qui est destinée au serveur du Monde. En accédant à tous les commentaires publiés sous cet article, Alice accède du même coup au commentaire de Bob qui correspond à l'octet 01010101. Le serveur du Monde commence par stocker la requête d'Alice, puis l'exécute et, si le résultat informatique est correct, appelle la base de données du Monde qui stocke le commentaire de Bob auquel Alice demande l'accès. Une fois trouvé le commentaire de Bob dans sa base de données, le serveur du Monde envoie, à destination de l'ordinateur d'Alice, une requête qui confirme la bonne exécution de la requête d'Alice et qui, dans son champ, DATA comporte notamment le message de Bob auquel Alice accède. L'ordinateur d'Alice stocke la requête du Monde, puis l'exécute (y compris la donnée 01010101 de Bob), et voit ainsi s'afficher le message de Bob.



En l'espèce, l'octet 01010101 (le message de Bob) possède une échelle de diffusion qui s'étend à trois machines différentes : une machine qui a produit cette donnée (le smartphone de Bob) ; et trois machines qui l'ont stockée (le smartphone de Bob, le serveur du Monde et l'ordinateur d'Alice). Couvrant trois machines différentes, l'échelle de diffusion est ainsi constituée : d'une échelle de production s'élevant à une seule machine ; et d'une échelle de stockage s'élevant à trois machines différentes⁵³⁴. L'échelle de diffusion d'une donnée s'évalue dans le temps par le nombre total de machines différentes qui ont produit ou stocké cette donnée durant la période évaluée (par exemple le nombre de machines différentes qui ont produit la donnée 01010101, donc un message identique à celui de Bob, et/ou qui l'ont stockée entre le 1^{er} janvier 2021 et le 31 décembre 2021).

Les seuls êtres humains qui peuvent directement alimenter une échelle de diffusion sont les prescripteurs numériques – ces derniers étant précisément définis comme les personnes capables de produire ou de stocker des données exécutables par une machine numérique. Dans notre exemple, la donnée 01010101 n'a pu gagner son échelle de diffusion que par les transferts de données entre les utilisateurs Bob et Alice, les fabricants des machines de Bob, d'Alice et du Monde, les programmeurs des systèmes d'exploitation de Bob, Alice et du Monde, les programmeurs de l'application Le Monde, l'administrateur du serveur du Monde (qui met à disposition son serveur) et le propriétaire de l'application Le Monde (qui met à disposition des autres prescripteurs les données constitutives de ses programmes). Par conséquent, **les rapports de force interhumains en ligne contribuent à l'échelle de diffusion d'une donnée grâce à l'échange de données entre les machines de prescripteurs numériques**. Pour réguler l'échelle de diffusion d'une donnée, telle que cette échelle résulte de rapports de force interhumains en ligne, on s'assurera donc de contrôler les échanges (*i.e.* les transferts et transmissions de données) entre les prescripteurs numériques. À ce stade, on connaît donc le système qu'on cherche à réguler – l'échelle de diffusion d'une donnée –, ainsi que les composants de ce système dont on cherche

⁵³⁴L'exemple est évidemment simplifié ici. Par exemple, on doute que l'application du Monde soit hébergée sur le même serveur que la base de données des commentaires publiés sur Le Monde. De même, le commentaire de Bob est peut-être stocké en cloud, le Monde utilise peut-être des serveurs supplémentaires pour utiliser des logiciels SaaS de gestion des commentaires etc. Le message de Bob aurait donc, en réalité, une échelle de diffusion probablement supérieure à celle indiquée ici, car elle serait stockée sur de nombreux serveurs.

à contrôler les échanges – les transferts et transmissions de données entre prescripteurs numériques⁵³⁵.

3/ Quelle perturbation du système cherche-t-on à éliminer par la régulation ? Dans le cadre de cette thèse, la perturbation du système (*i.e.* de l'échelle de diffusion) qu'on cherche à éliminer est **l'inefficacité des normes juridiques sur l'échelle de diffusion d'une donnée**. Évaluer cette inefficacité nécessite de distinguer les données dont le régulateur souhaite réduire l'échelle de diffusion par rapport aux données dont il souhaite maintenir voire augmenter l'échelle de diffusion. En effet, le régulateur juridico-étatique peut se positionner de deux manières face à l'échelle de diffusion d'une donnée : il peut refuser qu'une donnée conserve ou amplifie son échelle de diffusion (on parlera de *Rejected-DATA*, ou R-DATA) ; ou il peut au contraire admettre qu'une donnée conserve ou amplifie son échelle de diffusion (on parlera d'*Admitted-DATA*, ou A-DATA).

Une R-DATA peut par exemple désigner une donnée rendue illégale, inconstitutionnelle ou contraire à la jurisprudence par le régulateur, ou encore une donnée qui n'est pas explicitement qualifiée comme contraire au droit positif mais dont le régulateur s'efforce manifestement de réduire l'échelle de diffusion. Ainsi, pour reprendre notre illustration fictive, l'octet 01010101 (message publié par Bob) peut être qualifié de R-DATA en France, car un tel message est contraire à la loi du 29 juillet 1881 sur la liberté de la presse⁵³⁶. Inversement, une A-DATA est une donnée dont le régulateur ne cherche pas à réduire l'échelle de diffusion, voire une donnée dont le régulateur cherche à augmenter l'échelle de diffusion. Par exemple, le simple clic sur une souris ou un écran tactile correspond à une donnée. Le stockage de cette seule donnée n'est contraire à aucune ambition du régulateur, car tous les États qui autorisent l'utilisation d'internet admettent par définition que les utilisateurs puissent cliquer, donc produire ou stocker la donnée correspondant au clic. La donnée qui résulte de la seule action du clic est alors un A-DATA.

Le périmètre d'une R-DATA est délimité par le régulateur : par essence, lui seul peut définir les données qu'il refuse. Une R-DATA peut donc tout à fait concerner une donnée très spécifique (par exemple l'octet 01010101), tout comme elle peut couvrir un ensemble de données rassemblées en une catégorie. Sont ainsi qualifiables de R-DATA les catégories « publication de propos haineux », « cyberharcèlement », « intrusion dans un système informatique à l'aide d'un logiciel malveillant », « diffusion de fausses informations », « consommation illicite de biens culturels », « production et stockage de contenus pédopornographiques », « vol de données » etc. Par opposition, toutes les données qui ne sont pas refusées par le régulateur sont des A-DATA. On insiste sur l'importance de cette délimitation des R-DATA par le régulateur,

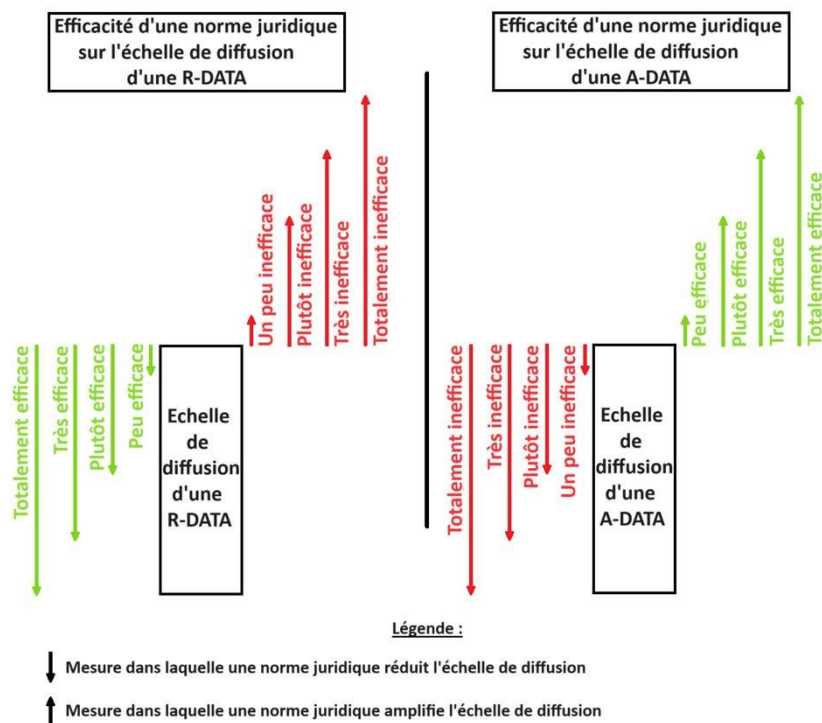
⁵³⁵On appelle « transferts de données » les mouvements de données locaux, *i.e.* ceux qui se produisent à l'intérieur de la machine (transfert d'une donnée entre la mémoire vive et le processeur, ou entre tel et tel registre du processeur, ou entre la carte graphique et la mémoire vive etc.). On appelle « transmissions de données » les mouvements de données externes, *i.e.* ceux qui consistent à faire stocker par une machine B des données émises par une machine A (transmission de données entre un terminal et un routeur, entre un routeur et un serveur, entre un routeur et un objet connecté, entre deux terminaux par Bluetooth...).

⁵³⁶Un tel message est en effet constitutif d'une diffamation (art. 29 de la loi de 1881, dès lors que Bob s'appuie sur des faits – inexacts ici – pour porter atteinte à la considération des arabes) et d'une provocation à la discrimination et à la haine (art. 24, al. 7 et 8, sachant qu'il n'est pas nécessaire que le propos ait appelé ou incité à la commission d'actes pourvu que le propos « *suscite un sentiment de rejet ou d'hostilité, la haine ou la violence envers un groupe de personnes à raison d'un critère discriminant évoqué à l'art. 24* » - v. p. ex. C. Cass., crim., 1^{er} fév. 2017, n° 15-84.511)

pour que ce dernier puisse cibler très exactement la donnée ou la catégorie de données contre laquelle il emploie des techniques de régulation.

On verra plus loin quels sont les effets contraires dont le déséquilibre provoque l'inefficacité des normes juridiques sur une échelle de diffusion, et comment corriger ce déséquilibre afin d'éliminer cette inefficacité. Toutefois, on peut déjà à ce stade définir notre méthode pour mesurer l'inefficacité d'une norme juridique sur l'échelle de diffusion d'une donnée. Si le régulateur souhaite réduire l'échelle de diffusion d'une donnée, c'est-à-dire en présence d'une R-DATA, on estimera qu'une norme juridique est efficace si elle parvient à réduire l'échelle de diffusion de cette R-DATA ; on la tiendra en revanche pour inefficace si elle n'y parvient pas, voire si elle n'empêche pas une augmentation de l'échelle de diffusion de la R-DATA. Inversement, si le régulateur souhaite maintenir ou augmenter l'échelle de diffusion d'une donnée, c'est-à-dire en présence d'une A-DATA, on estimera qu'une norme juridique est efficace si elle parvient à maintenir ou à augmenter l'échelle de diffusion de cette A-DATA ; on la tiendra pour inefficace si

elle n'y parvient pas, voire si elle n'empêche pas une réduction de l'échelle de diffusion de la A-DATA. Dès lors, **une norme juridique est plus ou moins efficace sur une échelle de diffusion selon la mesure dans laquelle cette norme réduit l'échelle de diffusion d'une R-DATA ou maintient/amplifie l'échelle de diffusion d'une A-DATA ; elle est plus ou moins inefficace selon la mesure dans laquelle cette norme augmente l'échelle de diffusion d'une R-DATA, ou réduit l'échelle de diffusion d'une A-DATA.**



Section 2. Les types de restriction d'accès selon la source de la restriction

On commence par examiner les techniques de régulation par restriction de l'accès à une donnée. Les techniques de restriction seront distinguées selon qu'elles sont pratiquées : depuis la transmission de données (Paragraphe 1) ; ou depuis le stockage de données (Paragraphe 2).

Paragraphe 1 – La restriction de la transmission de données

Seront ici abordés deux techniques de restriction de l'accès depuis la transmission de données = la coupure de l'accès (A) et le ralentissement de l'accès (B).

A) *La coupure de la transmission*

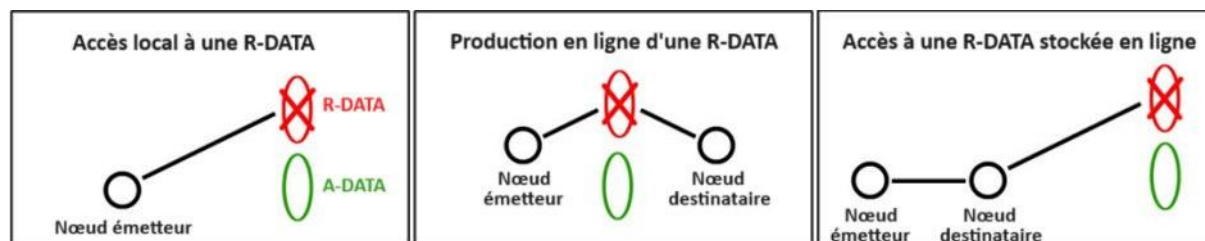
Compte tenu de la différence entre réalités interne (endogène) et externe (exogène) à la machine, on subdivise la régulation de machines connectées en deux sortes de régulation. Premièrement, les règles que le régulateur cherche à faire respecter peuvent être comprises par la machine, auquel cas on parlera de « régulation interne » pour désigner l'ensemble de ces règles comprises par la machine. Deuxièmement, les règles que le régulateur cherche à faire respecter peuvent être comprises par les seuls êtres humains à l'exclusion de la compréhension machinale, auquel cas on parlera de « régulation externe ». Les peines, les sanctions patrimoniales, civiles ou professionnelles, les dispositifs incitatifs ou désincitatifs sont autant d'instruments de régulation externe qui s'appliquent à des conditions humaines (sociales, économiques, de déplacement, de motivation...).

Toutefois, étudier l'efficacité de la régulation externe demande de connaître les lois externes à la machine qui régissent les agents sociaux humains. Or, un tel examen sort du cadre de notre travail focalisé sur les lois internes à la machine telles qu'on les a identifiées (neutralité et interopérabilité exécutives, solidarité applicative, interconnexions binaire, protocolaire et opérationnelle), qui régissent la création, la réalisation et la persistance des données stockées sur le réseau internet. Par conséquent, on ne sera pas en mesure d'évaluer l'efficacité de l'action régulatrice externe. **Notre étude de l'efficacité de l'action régulatrice se concentrera alors sur la régulation interne**, comprise par la machine. On catégorisera ici les diverses techniques de régulation du réseau internet en illustrant la façon dont elles peuvent être juridiquement utilisées par l'État.

Précisément, on catégorise ces techniques de régulation selon le critère de « l'accès à des données par une ou plusieurs machines connectées ». Le choix de ce critère s'explique par le fait qu'on étudie ici la régulation de l'échelle de diffusion concrète d'une donnée. En effet, l'accès à une donnée (*i.e.* sa production ou son stockage dans le cadre d'une requête) est l'action qui a immédiatement pour effet de provoquer l'exécution de cette donnée par la machine. Dès lors que l'échelle de diffusion (concrète) d'une donnée est constituée par le nombre de machines différentes qui l'exécutent, cette échelle est alimentée par toutes les machines différentes qui produisent ou stockent cette donnée dans le cadre d'une requête. Le régulateur peut donc faire varier les échelles de diffusion en empêchant l'accès à une R-DATA ou en favorisant l'accès à une A-DATA. Pour cette raison, **on classe les techniques de régulation selon le type de relation qu'établit une technique entre le nœud émetteur qui requiert l'exécution d'une R-DATA ou A-DATA et le nœud récepteur de cette requête**. Ainsi, comme on s'apprête à le détailler, l'accès à une R-DATA peut être empêché grâce à plusieurs types de relations entre le nœud émetteur et le nœud récepteur, tout comme l'accès à une A-DATA peut être favorisé grâce à plusieurs types de relation entre ces nœuds. On définit le nœud d'un réseau comme toute unité membre de ce réseau.

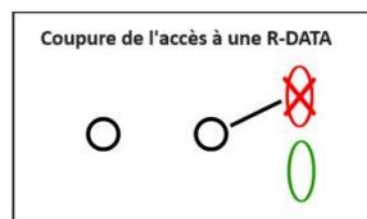
On s'attardera d'abord sur les techniques de régulation par restriction de l'accès aux R-DATA, avant d'étudier plus loin les techniques de régulation par augmentation de l'accès à la A-DATA. On identifie trois configurations d'accès à une R-DATA. Un prescripteur peut d'abord accéder à une R-DATA localement sur sa propre machine. Dans ce cas, la R-DATA stockée sur sa machine est le fruit des instructions des programmes locaux que le prescripteur combine et dont il ordonne l'exécution. Un prescripteur peut ensuite ordonner l'exécution, *sur le réseau*, d'une R-DATA qu'il a lui-même produite. Dans ce cas, sa requête est porteuse d'une R-DATA exécutée par la machine destinataire (publication d'un propos haineux, diffusion d'un logiciel

malveillant, dépôt illégal sur internet d'une oeuvre protégée...). Un prescripteur peut enfin accéder à une R-DATA déjà stockée sur internet. Dans ce cas, il ne produit pas lui-même la R-DATA mais en ordonne l'exécution par la machine qui héberge cette R-DATA et par sa propre machine (consultation d'un propos haineux, téléchargement d'un logiciel malveillant, consommation illicite d'une oeuvre protégée...).



Pour restreindre l'accès à une R-DATA – local ou par un tiers –, il est possible d'agir sur deux types de machines connectées en l'état du réseau internet : celles qui ont pour rôle de transmettre les données (infrastructures réseau) ; et celles qui ont pour rôle de stocker les données transmises et à transmettre (terminaux, serveurs et périphériques accessoires). Les pages qui suivent se focalisent sur la restriction de l'accès à une R-DATA dès la transmission, nous aborderons ensuite la restriction de l'accès à une R-DATA dès le stockage.

La première technique de restriction de la transmission qu'on identifie est la coupure. On appelle « coupure de l'accès à une R-DATA » la technique qui consiste à interrompre provisoirement ou définitivement la connectivité entre le nœud émetteur et le nœud destinataire qui stocke les données aboutissant à une R-DATA. La relation établie par la coupure entre le nœud émetteur et le nœud destinataire prend donc la forme d'une absence de connectivité : le nœud destinataire stocke les données nécessaires à la réalisation de la R-DATA, mais le nœud émetteur ne peut accéder à ces données (i.e. ne peut ni les produire ni les stocker, donc ne peut pas contribuer à leur échelle de diffusion).



La coupure peut être pratiquée sur les moyens de transport aussi bien que sur ceux d'acheminement. Du côté des moyens de transport, on rappelle que de nos jours ces moyens peuvent être sous-marins (câbles), terrestres (câbles), aériens (antennes, bornes, Bluetooth...) ou satellitaires. Par exemple, la coupure menace souvent les câbles sous-marins. Généralement conçus avec la technologie de la fibre optique et transportant 99% du trafic internet⁵³⁷, ces câbles sont l'objet de vives tensions entre les États qui cherchent à assurer leur autonomie économique et technologique mais aussi leur hégémonie géopolitique face à aux autres États⁵³⁸.

⁵³⁷« Cartographie. Le long des câbles sous-marins, sur les routes de l'information », *Courrier international* [en ligne], 3 sept. 2018. La fibre optique est une technologie filaire (câbles) qui transporte des signaux de lumière. Ces câbles représentent un progrès dans la vitesse du transport par rapport aux câbles électriques qui transportent des signaux électriques. Un câble électrique transporte les signaux à la vitesse du courant électrique (200 000 km/s) tandis que la fibre optique les transporte à la vitesse de la lumière (299 792 km/s). La fibre optique exploite donc des ondes hertziennes (la lumière), les câbles électriques exploitent le courant électrique.

⁵³⁸Sur le plan économique, si le marché du transport est monopolisé par un État, les autres États peuvent eux aussi souhaiter tirer profit de ce marché et en acquérir une ou plusieurs parts. Sur le plan

Le droit international de la mer reconnaît à tout État Partie aux conventions la liberté de poser et de gérer de tels câbles, mais leur interdit de porter atteinte à l'intégrité des câbles appartenant à un autre État et de perturber le système de communication de l'État côtier⁵³⁹. De la liberté de l'État de poser et de gérer des câbles découle celles de ne pas en poser et de les gérer selon ses intérêts, donc de couper l'accès sous-marin à son territoire par des réseaux étrangers. Les États tiennent donc du droit international la liberté de couper l'accès sous-marin à leur réseau national, sous réserve de ne pas s'immiscer dans la liberté qu'ont les autres États de gérer leur accès sous-marin⁵⁴⁰.

En 2022, quatre pays ne sont connectés à aucun câble sous-marin : le Salvador, le Monténégro, la Slovaquie et la Corée du Nord. Seuls les trois premiers pays ont ratifié la convention de Montego Bay sur le droit de la mer de 1982, tandis que la République populaire démocratique de Corée (Corée du Nord) en est seulement signataire sans l'avoir reconnu dans son

technologique, si un État connecte à lui seul tous les autres États, les données transportées sur le sol de ces États et par leurs résidents dépendent de la gestion du transport effectuée par l'État monopolisateur. Sur le plan géopolitique, si un État exerce une hégémonie technologique sur d'autres États, cette situation hégémonique crée diverses dépendances des États assujettis au profit de l'État hégémonique (agenda du développement technique défini par l'hégémon, autorités scientifiques des États, équilibre des puissances étatiques...). D'abord britannique du dernier quart du XIX^e siècle jusqu'aux années 1950, l'hégémon est devenu américain avec l'essor d'AT&T dans les années 1960, lequel hégémon américain se voit de plus en plus concurrencé par les fabricants et investisseurs chinois de câbles sous-marins (Hengtong, Huawei Marine, Baidu, Alibaba, Tencent...). V. MOREL Camille, *L'État et le réseau mondial de câbles sous-marins de communication*, Thèse de droit de l'université de Lyon, 2020, p. 210s. [en ligne sur gouvernement.fr]

539 Sur la liberté de la pose de câbles sous-marins, en zone exclusive économique (économiquement exploitable par le seul État côtier) comme en haute mer (eaux internationales soumises à des règles de respect mutuel entre États) : Convention sur la haute mer du 29 avril 1958 [63 États parties, 46 signataires], art. 2, 3) et Convention des Nations Unies sur le droit de la mer du 10 déc. 1982 [« Convention de Montego Bay sur le droit de la mer », 168 États parties, 158 signataires], art. 58, 79, 87, c) et 112. Sur l'interdiction de porter atteinte à l'intégrité des câbles appartenant à un autre État : Convention sur la haute mer de 1958, art. 26 à 29, et Convention de Montego Bay sur le droit de la mer, art. 51§2 et 113. Sur l'interdiction de perturber le système de communications de l'État côtier : Convention sur la haute mer, art. 27 ; Convention de Montego Bay sur le droit de la mer, art. 19§2 k)

⁵⁴⁰ Au début de l'invasion russe en Ukraine, s'est posée la question de savoir si la Russie pourrait « sectionner » les câbles sous-marins qui connectent directement le continent américain au continent européen (CARASSIO Joël, « Guerre en Ukraine. Câbles sous-marins », *DNA.fr* [Dernières Nouvelles d'Alsace], mars 2022.). Elle peut probablement le faire techniquement, à l'aide de « *mini sous-marins de plongée profonde à propulsion nucléaire (...) connus sous le terme russe AGS* » équipés de « *bras manipulateurs pour travailler sur les câbles* » (DELEURY Patrick, « Comment les sous-marins d'espionnage russes peuvent interférer avec les câbles Internet sous-marins - AGASM-Sous-marins sous-marin », sur AGASM.fr [Association Générale des Amicales de Sous-Marinières], publié le 20 août 2020). Mais la Russie ne peut pas le faire sans violer le droit international, *i.e.* sans violer la compétence de tous les États sur la gestion des câbles reliés à leur territoire, et donc sans provoquer une crise géopolitique mondiale absolument majeure. Dans les faits, les conséquences seraient tout à fait mineures. D'une part, au lieu d'emprunter un câble reliant directement l'Europe et les États-Unis, les paquets de données échangés entre ces deux territoires emprunteront un autre trajet avec correspondance (par ex., les paquets provenant de la France pourraient emprunter le câble sous-marin SeaMea3 qui relie la France et la Corée du Sud puis le câble New Cross Pacific Cable System qui relie la Corée du Sud et les États-Unis, ou pourraient emprunter le câble Asia Africa Europe-1 qui relie la France à la Chine puis le câble FASTER qui relie la Chine aux États-Unis). D'autre part, les paquets étant transmis à la vitesse de la lumière, la répercussion de ce changement de trajet sera moindre sur la vitesse de la transmission.

droit positif interne – *i.e.* sans en être partie. Dans le cas de la Corée du Nord, la coupure semble être un choix de l'État⁵⁴¹. La Corée du Nord coupe toute connexion sous-marine des machines situées sur son territoire avec les machines connectées en-dehors de son territoire. En rendant impossible le transport sous-marin vers ou depuis des machines étrangères, l'État nord-coréen pratique une coupure de l'accès à la R-DATA « données étrangères ». Ici, la coupure pratiquée auprès des câbles sous-marins sert donc à empêcher l'accès des nord-coréens à la R-DATA « données stockées hors Corée du Nord ». Les machines étrangères peuvent toujours stocker la R-DATA et y accéder, mais les machines situées en Corée du Nord ne peuvent y accéder par voie sous-marine faute de connexion sous-marine avec les machines étrangères.

La coupure peut concerner n'importe quelle installation de transport (terrestre, aérien, satellitaire) autre que les câbles sous-marins. Comme pour les câbles sous-marins, le droit international des télécommunications protège les installations de chaque État contre les ingérences d'autres États : il interdit aux 193 États membres (dont la Corée du Nord) de brouiller les transmissions hertziennes sur le territoire d'un autre État membre, de perturber par leurs propres appareils et installations le fonctionnement de ceux situés sur le territoire d'un autre État membre, et de dépasser les limites de leur juridiction dans le cadre de la gestion de leurs appareils et installations⁵⁴².

La transmission des télécommunications obéit au principe selon lequel « *les États doivent prendre les mesures utiles en vue d'établir, dans les meilleures conditions techniques, les voies et installations nécessaires pour assurer l'échange rapide et ininterrompu des télécommunications internationales* »⁵⁴³. Cependant, d'importantes exceptions dérogent à ce principe. Un État membre peut interrompre la transmission de télécommunications « *qui paraîtraient dangereuses pour la sûreté de l'État ou contraire à ses lois, à l'ordre public ou aux bonnes mœurs* », et peut même suspendre son service national de télécommunications « *soit de manière générale, soit seulement pour certaines relations ou pour certaines natures de correspondances* » sans avoir à se justifier d'une quelconque raison ayant conduit à cette suspension⁵⁴⁴. Tant pour les câbles sous-marins que pour n'importe quel autre moyen de transmission des données sur internet, le droit international reconnaît donc à tout État la pleine liberté de pratiquer des coupures à condition de ne pas s'ingérer dans la juridiction d'autres États. Par exemple, la Corée du Nord ne coupe pas seulement l'accès sous-marin à son réseau national de télécommunications, mais coupe par ailleurs tout accès aérien étranger au moyen de brouilleurs-radio employés par l'Armée populaire de Corée aux frontières⁵⁴⁵. De cette façon, est empêché la transmission de tout appel téléphonique étranger, de toutes données transportées par des antennes étrangères, de tout accès radio au territoire nord-coréen. Les seuls moyens de transport permettant d'accéder au réseau nord-coréen sont les voies terrestre (connexion à la Russie et à Hong-Kong par l'acheminement) et satellitaire (connexion à l'Allemagne par satellite grâce à des serveurs

541 On suppose qu'il s'agit d'un choix en raison de la stratégie d'isolement de l'État en Corée du Nord qui, contrairement au Monténégro, à la Slovénie ou au Salvador, tient les données étrangères pour des R-DATA interdites d'accès comme on l'observera

542 Constitution de l'Union Internationale des Télécommunications, respectivement art. 45, art. 38§5 et art. 38§3

543 *Ibid.*, art. 38§1

544 *Ibid.*, art. 34 et 35

545 « North Korea: Connection Denied: Restrictions on mobile phones and outside information in North Korea » [en ligne], *Amnesty International*, 9 mars 2016, p. 34

nord-coréens situés à Berlin et appartenant au Korea Computer Center⁵⁴⁶). Le cas nord-coréen illustre l'extrême souplesse du principe international de « *l'échange rapide et ininterrompu des télécommunications internationales* », que la Corée du Nord ne viole pas en coupant tout accès sous-marin et aérien de son réseau national à des réseaux étrangers. Les restrictions nord-coréennes sont pleinement compatibles avec le droit international des télécommunications dès lors que l'État justifie ces restrictions par la sûreté publique ou les bonnes mœurs (il n'est d'ailleurs même pas obligé de se justifier comme on l'a vu). En effet, c'est par protection de la moralité, de la sûreté et de l'ordre publics que les articles 183, 184 et 185 du Code pénal nord-coréen de 2015 condamnent la conservation, la diffusion et l'accès à tout « *acte et culture décadents ou hostiles* »⁵⁴⁷.

Outre les moyens de transport, la coupure de l'accès à une R-DATA peut aussi être pratiquée auprès des moyens d'acheminement, *i.e.* les routeurs IP et passerelles. En France, la première version de la loi Hadopi de 2009 confiait à la Haute autorité pour la diffusion des

⁵⁴⁶ À l'issue d'un appel d'offre nord-coréen opposant des fournisseurs chinois et le riche homme d'affaire allemand Jan Holtermann en 2003, ce dernier a remporté le marché pour établir une première connexion du réseau nord-coréen avec un réseau étranger (allemand en l'espèce). Ancien employé de l'ambassade nord-coréenne à Berlin, J. Holtermann a investi 1 milliard de dollars pour l'installation dans la capitale allemande de serveurs connectés à un satellite retransmettant les requêtes provenant de ce serveur vers des serveurs en Corée du Nord. J. Holtermann a obtenu le marché dans le cadre de l'entreprise KCC Europe qu'il a préalablement fondé, l'une des quatre filiales du Korea Computer Center avec celles en Chine, en Syrie et aux Émirats arabes unis (BANKS Stacey, « North Korean Telecommunications », *North Korean Review*, 1, McFarland & Company, vol. 1, 2005, p. 93).

⁵⁴⁷ L'article 183 (« Importation et diffusion de culture décadente ») prévoit : « *toute personne qui importe sans autorisation, crée, diffuse ou stocke illégalement du matériel au contenu décadent, érotique et vulgaire, tel que des dessins, des photographies, des livres, des chansons ou des films, sera condamnée à une peine de rééducation par le travail de moins d'un an. / Dans les cas où l'importation, la création, la diffusion ou le stockage a eu lieu plusieurs fois ou en grande quantité, la personne sera condamnée à une peine de rééducation par le travail inférieure à 5 ans. / Dans les cas graves, elle sera condamnée à une peine de rééducation par le travail de plus de 5 ans et de moins de 10 ans.* ». L'article 184 (« Commission d'actes décadents ») prévoit : « *toute personne qui a vu ou écouté des actes reproduits qui reflètent un contenu décadent, érotique et vulgaire, tels que des dessins, des photographies, des livres, des chansons ou des films, sera condamnée à une peine de rééducation par le travail de moins d'un an. / Si la personne a commis de manière habituelle les actes visés au paragraphe précédent, elle sera condamnée à une peine de rééducation par le travail inférieure à 5 ans. / Dans les cas graves, elle sera condamnée à une peine de rééducation par le travail de plus de 5 ans et de moins de 10 ans.* ». L'article 185 (« Écoute d'émissions hostiles et collecte, stockage, diffusion de biens hostiles ») prévoit : « *toute personne qui a écouté des émissions ennemies ou qui a collecté, stocké ou diffusé des biens hostiles sans but contre la Nation sera condamnée à une peine de rééducation par le travail de moins d'un an. / Dans le cas où la personne a commis habituellement les actes prévus au paragraphe précédent ou a collecté, stocké ou diffusé une grande quantité de biens hostiles, elle sera condamnée à une peine de rééducation par le travail inférieure à 5 ans. / Dans les cas graves, elle sera condamnée à une peine de rééducation par le travail de plus de 5 ans et de moins de 10 ans.* ». Ces informations sont disponibles sur la base de données unilaw.go.kr. Cette base de données est constituée par les ministères sud-coréens de la Réunification, de la Justice et de la Législation gouvernementale, dans le but notamment de rendre accessible la culture légale nord-coréenne. Le site internet lawandnorthkorea.com répertorie et simplifie la lisibilité des données d'unilaw.go.kr, en traduisant en anglais les documents rassemblés, dans le but d' « *offrir aux chercheurs la possibilité de mener des recherches juridiques contemporaines sur deux juridictions ayant une histoire, une culture et une langue communes, mais une politique moderne très différente* ».

œuvres et la protection des droits sur internet⁵⁴⁸ le pouvoir de requérir des opérateurs qu'ils coupent provisoirement toute possibilité de connexion au réseau internet des personnes accusées par l'autorité d'avoir téléchargé illégalement des œuvres protégées depuis des services de communication au public en ligne. Pour effectuer une coupure depuis ses moyens d'acheminement, l'opérateur peut par exemple désactiver le routeur passerelle (box internet, modem...) auquel est connecté l'abonné sanctionné. Le Conseil constitutionnel a néanmoins censuré ces dispositions, considérant que la coupure de la connexion pour de tels motifs et sous de telles modalités était contraire à la « *liberté d'accéder aux services de communication au public en ligne* » découlant de la liberté d'expression (art. 2 de la Déclaration des droits de l'Homme et du Citoyen de 1789)⁵⁴⁹. Par-là, tout en reconnaissant que ce droit n'est pas absolu, le Conseil consacre le « *droit [pour chacun] de se connecter à l'internet* »⁵⁵⁰, et interdit donc en principe le recours par l'État à la technique de la coupure.

De nombreux États recourent à des coupures temporaires, notamment en Afrique, au Moyen-Orient, en Amérique centrale et en Asie. Le record de longévité d'une coupure temporaire est de 19 mois en Birmanie (entre juin 2019 et février 2021), dont le gouvernement a coupé la connexion au réseau internet dans les zones en proie à la guérilla (régions de Chin et de Rakhine)⁵⁵¹. Sur le continent africain, le record de longévité est détenu par le Cameroun, qui a coupé toute connexion entre les machines situées au Cameroun anglophone (Est du Cameroun) et les machines situées à l'extérieur de cette région pendant 93 jours (du 19 janvier au 20 avril 2017), lors d'une guerre civile opposant le Cameroun francophone majoritaire partisan de l'application du droit civil et le Cameroun anglophone minoritaire partisan de l'application du *common law* dans les juridictions camerounaises⁵⁵². La coupure est employée pour des raisons assez diverses. Elle est le plus souvent mobilisée pour éviter qu'un conflit social ne s'amplifie sur internet⁵⁵³. Les États peuvent aussi y recourir pour retirer provisoirement ou définitivement aux

548La Hadopi est devenue l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) par fusion avec le Conseil Supérieur de l'Audiovisuel en 2022 (loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique)

549Conseil Constitutionnel français, 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet* (HADOPI 1), n° 2009-580 DC, cons. 12

550Conseil constitutionnel français, Commentaire de la décision n° 2009-580 DC, p. 6

551« Birmanie : coupure internet dans les États de Rakhine et de Chin », *Radio France internationale*, 22 juin 2019 [en ligne]

552GRAS Romain, « Cameroun : une plante déposée contre l'État pour dénoncer les coupures Internet en zone anglophone », *Jeune Afrique*, 31 janv. 2018 [en ligne]

553Par exemple, lors de la révolution de 2011, l'Égypte avait ordonné aux opérateurs de cesser de fournir leurs services d'accès au réseau internet durant cinq jours (l'État était alors parvenu à couper environ 88% du réseau accessible en Égypte, v. « La coupure d'Internet en Égypte, une première mondiale par son ampleur » [en ligne], *Libération*, 28 janv. 2011). En 2019, l'Indonésie a interrompu toute connexion durant un peu moins de 24h dans sa région de Papouasie occidentale à l'occasion d'émeutes survenues après l'arrestation de 43 étudiants papous et une manifestation contre la présence d'étudiants papous (« Des manifestations dégénèrent en émeutes dans la province indonésienne de Papouasie occidentale » [en ligne], *Le Monde*, 21 août 2019). En février 2021, l'Inde a coupé l'accès à internet durant une demi-journée dans les environs de New Delhi, 48h dans trois autres zones aux frontières de Delhi et dans 14 des 22 districts de l'État d'Haryana après un affrontement entre agriculteurs et policiers (MITRA Esha, HOLLINGSWORTH Julia, « India cuts Internet around New Delhi as protesting farmers clash with police » [en ligne], *CNN*, 3 fév. 2021)

territoires étrangers tout droit de regard sur leur réseau national⁵⁵⁴. Ils y recourent aussi parfois pour isoler des régions et minorités discriminées⁵⁵⁵, ou encore des opposants politiques⁵⁵⁶. Plus original, en Algérie depuis 2017, l'État coupe la connexion internet dans tout le pays pendant cinq jours chaque année, afin d'éviter que les lycéens utilisent le réseau internet pour tricher au baccalauréat durant les cinq jours de l'épreuve⁵⁵⁷.

La coupure a ses avantages et ses inconvénients pour la réduction de l'échelle de diffusion d'une R-DATA sur le territoire d'un État. Quant à ses avantages, cette technique ne peut être contrecarrée qu'en installant clandestinement des infrastructures-réseau (routeurs, câbles, bornes, antennes... non contrôlés par l'État) qui nécessitent des moyens économiques et techniques importants, à la mesure de la taille du réseau clandestin. Difficile à contourner, cette technique peut donc se révéler très efficace pour réduire l'échelle de diffusion d'une R-DATA sur le territoire étatique, et ainsi pour cloisonner le réseau internet dans des limites géographiques.

Quant à ses inconvénients, la coupure interrompt la totalité du trafic et non une catégorie de contenus (illicites), de programmes (malveillants) ou de services. L'État qui coupe la connexion entre deux machines ne pourra pas empêcher spécifiquement l'accès à un type de contenus, de programmes ou de services mais empêchera l'accès à tous les contenus, programmes et services auxquels le trafic permet l'accès. La coupure n'est donc pertinente que si la R-DATA dont l'accès est coupé couvre un trafic entier – tel que la R-DATA « données étrangères » qui couvre tout le trafic étranger. *A contrario*, si la R-DATA contre laquelle est pratiquée la coupure ne couvre pas tout le trafic coupé (par ex., recours à la coupure pour empêcher l'accès aux services de consultation ou de téléchargement illicites d'œuvres protégées), cela se traduit nécessairement une coupure de l'accès à toutes les R-DATA et A-DATA auxquelles le trafic coupé offrait l'accès (contenus, programmes et services illicites comme licites stockés sur les machines étrangères auxquelles l'accès est coupé). On appelle « sur-coupure » la situation dans laquelle la coupure implique des A-DATA, *i.e.* la situation dans laquelle la coupure entraîne l'interruption de l'accès à des données admises par le régulateur (sites d'information et de commerces légaux, services et moyens d'échange autorisés...).

554Le 16 novembre 2019, lors d'une manifestation en Iran contre la hausse des prix de l'essence s'étant conclue par une centaine de morts par balles, le réseau internet est quasi-totalement coupé à l'intérieur du pays à l'exception des réseaux bancaires et gouvernementaux (« Iran. Coupure volontaire d'Internet pendant la répression meurtrière des manifestations de novembre 2019 – nouvelles investigations » [en ligne], sur *Amnesty International*, Communiqué de presse, 16 nov. 2020). Il est alors devenu impossible pour un regard extérieur de connaître le déroulement de la manifestation par le biais d'internet.

555Par exemple en Éthiopie, où l'État coupe quasi-totalement le réseau internet dans la région du Tigré depuis le début de la guerre le 4 novembre 2020 v. « Entretien sur la crise dans la région du Tigré en Éthiopie », *Human Rights Watch* [en ligne], juil. 2021 ; et HOLZINGER Flavie, RUBRICE Lucie, SIMONNET Victor et DEDIER Eric, « Couper Internet, une arme pour les régimes autoritaires africains », *Le Monde.fr*, janvier 2022

556C'est par exemple le cas en Biélorussie, à Cuba (« Survivre à une coupure d'internet », *La Quadrature du Net*, 21 avr. 2022 [en ligne]), ou encore au Congo où chaque mobilisation de l'opposition suscite des coupures depuis 2018 (« Coupures d'Internet en RDC », sur *TV5MONDE* [en ligne], 24 fév. 2018)

557Cette habitude annuelle est la conséquence d'une fuite massive des sujets sur le réseau internet durant la session du baccalauréat de 2016. V. LABEYRIE Isabelle, « Coupures d'internet et peines de prison ferme : les méthodes contre la triche au bac en Algérie », *France Info*, 24 juin 2021 [en ligne]

L'un des risques de la sur-coupure à long terme est celui d'un contournement de la coupure par l'emprunt de réseaux clandestins à l'image des anciennes radio-pirates. On l'a par exemple récemment observé en Ukraine : dès le début de l'invasion russe le 24 février 2022, le réseau de satellites d'accès internet emprunté par les Ukrainiens est victime d'une cyberattaque, qui entraîne une panne du transport satellitaire en Ukraine et dont l'Union Européenne et les États-Unis suspectent qu'elle a été commandée par l'État russe (la cyberattaque s'est diffusée une heure avant les premiers bombardements)⁵⁵⁸. Pour contourner la coupure du trafic des données ukrainiennes vers l'internet mondial, plus de 150 000 ukrainiens ont emprunté le réseau satellitaire Starlink fourni par l'entreprise SpaceX après que le PDG de SpaceX, Elon Musk, ait ordonné la distribution gratuite de kits Starlink sur le sol ukrainien⁵⁵⁹. Néanmoins, le risque de contournement est faible dans les pays les plus pauvres ou qui attirent peu le regard du monde, et il est par ailleurs très relativisé si les moyens de restriction déployés pour la coupure sont conséquents comme on le verra. Outre le risque de contournement, le principal inconvénient de la sur-coupure est économique. Spécialisée dans la comparaison des VPN et l'étude des politiques restrictives en ligne, l'entreprise Top10VPN évalue le coût des coupures et autres restrictions à 1,5 milliards de dollars au Nigéria, à 1,9 milliards en Afrique sub-saharienne et à 5,45 milliards de dollars dans le monde en 2021⁵⁶⁰.

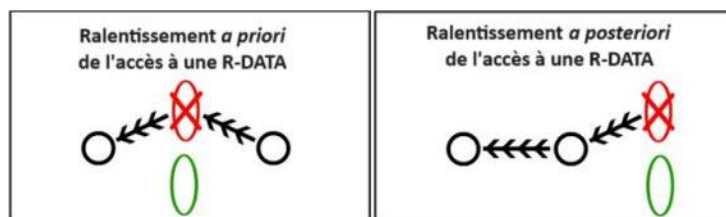
B) Le ralentissement de la transmission

En plus de la coupure, les infrastructures-réseau peuvent se voir appliquer une deuxième technique de restriction de l'accès : le ralentissement de l'accès à une R-DATA. On appelle « ralentissement de l'accès » la technique qui consiste, depuis le nœud émetteur, à ralentir le trafic en direction du nœud destinataire. L'usage du ralentissement par un opérateur ou un État est difficilement décelable car l'emploi de cette technique est peu ostensible et souvent imputable à d'autres causes qu'un ralentissement volontaire.

558« Les Occidentaux accusent la Russie d'avoir paralysé des satellites pour préparer l'invasion de l'Ukraine » [en ligne], *Le Figaro*, 10 mai 2022

559« Starlink. 150 000 Ukrainiens utiliserait le service internet par satellite d'Elon Musk », *Ouest France*, 3 mai 2022 [en ligne] ; « Comment le réseau Starlink permet à l'armée ukrainienne de résister face aux forces russes ? », *Siècle Digital* [en ligne], 14 juin 2022. Starlink est toutefois limité : en plus d'être particulièrement coûteuse (abonnement à 50-250€/mois et achat du matériel à 480-2500€ selon les pays et le type d'abonnement) et donc peu accessible dans les pays pauvres, l'utilisation de Starlink nécessite l'installation d'antennes paraboliques très ostentatoires et difficiles à dissimuler dans un régime autoritaire – d'autant que Starlink couvre aujourd'hui principalement l'hémisphère nord mais couvre minimalement les pays du sud (Starlink.com ; LAUSSON Julien, « SpaceX réduit fortement le prix de Starlink en France », *Numerama*, 3 août 2022 ; « Starlink Internet Review 2023: Plans, Pricing, and Speeds », *Satelliteinternet.com*, 10 mai 2023).

560« Combien les coupures d'internet ont coûté à l'Afrique subsaharienne en 2021 » [en ligne], *BBC News Afrique*, 15 janvier 2022



La configuration du ralentissement *a priori* désigne la situation dans laquelle le nœud destinataire (le plus souvent un routeur) ralentit la transmission d'une requête qui porte elle-même une R-DATA. Le ralentissement *a priori* est donc adapté lorsque le nœud émetteur est l'auteur de la R-DATA (publication de propos haineux, diffusion même involontaire d'une cyberattaque, partage illicite d'œuvres protégées...). La configuration du ralentissement *a posteriori* désigne la situation dans laquelle le nœud destinataire (le plus souvent un routeur) ralentit la transmission d'une requête qui souhaite accéder à une R-DATA déjà hébergée sur internet. Le ralentissement *a posteriori* est donc adapté lorsque le régulateur espère empêcher au nœud émetteur d'accéder à une R-DATA déjà présente en ligne (consultation de contenus haineux, accès à des sites suspects, malveillants ou de partage illicite d'œuvres protégées...).

Dans l'Union européenne, le principe de neutralité d'internet interdit aux opérateurs de discriminer l'acheminement des données selon l'identité de l'émetteur ou du destinataire, les contenus consultés, les services accédés ou les terminaux utilisés⁵⁶¹. En principe, les opérateurs européens ne peuvent donc pas accélérer l'accès à certains services ou contenus au détriment d'autres dont l'accès serait ralenti. Ce principe vise notamment à protéger celui de libre concurrence : en l'absence de la neutralité d'internet, les services en ligne les plus fortunés (Amazon, Alphabet, Meta...) peuvent rémunérer les opérateurs dans le but d'obtenir un meilleur accès, aux dépens des services en ligne les moins fortunés qui bénéficieront d'un accès de moindre qualité.

Aux États-Unis en revanche, la *Federal Communications Commission* (FCC) a levé depuis 2017 l'application de ce principe qu'elle avait consacré deux ans auparavant⁵⁶². La décision est prise par vote de la FCC, sous l'autorité de son président Ajit Varadaraj Pai (2017-2021) nommé par le Président Donald Trump et politiquement proche de ce dernier. Pour justifier la disparition de la neutralité d'internet, Donald Trump invoquait principalement l'argument selon lequel cette disparition permettrait aux opérateurs « *et à leurs investisseurs de gagner plus d'argent pour qu'ils régulent « naturellement » le réseau et le marché, tout en contribuant à l'innovation* »⁵⁶³. Dès lors, rien n'interdit les opérateurs américains de ralentir l'accès à tel ou tel service.

⁵⁶¹Règlement européen 2015/2120 dit « pour l'accès à un Internet ouvert », art. 3.3

⁵⁶²KANG Cecilia, « F.C.C. Repeals Net Neutrality Rules » [en ligne], *The New York Times*, 14 décembre 2017, [consulté le 14 août 2022].

⁵⁶³ESCORNE Charlotte, « Les enjeux de la neutralité du Net aux États-Unis », *Hérodote*, n° 177-178, 2020, p. 222

Le ralentissement peut consister pour les routeurs à placer certains paquets IP en attente d'acheminement afin de traiter les autres paquets prioritaires⁵⁶⁴, à faire emprunter aux paquets IP l'une des routes les plus longues pour parvenir à destination⁵⁶⁵, ou encore à utiliser des appareils perturbant l'environnement électromagnétique pour ralentir le transport hertzien. Par rapport à la coupure, **le ralentissement a pour avantage de rendre possible la restriction ciblée** de l'accès à tel ou tel service ou contenu depuis les moyens d'acheminement. Cette technique est alors nettement plus adaptée que la coupure pour restreindre des R-DATA constituées par des contenus, des services ou des programmes spécifiques (contenus haineux ou de cyberharcèlement, services jugés dangereux, programmes indésirables...). Le ralentissement a pour deuxième avantage notable de **prioriser le traitement de certaines requêtes** (non ralenties) au détriment d'autres (ralenties). Il peut par ailleurs décourager le prescripteur d'accéder à la R-DATA en consommant de son temps et de sa patience. Son principal inconvénient réside dans le fait que, contrairement à la coupure, **le ralentissement est assez aisément contournable** – on l'expérimentera *infra*. Le second inconvénient réside là encore dans le **risque de sur-ralentissement des A-DATA**. Le sur-ralentissement peut avoir pour conséquence d'accroître le risque de contournement du ralentissement (en impliquant parmi les victimes du ralentissement les prescripteurs qui accédaient aux A-DATA avant leur ralentissement et non pas seulement ceux qui accédaient aux R-DATA), et de pénaliser l'économie nationale par la faible qualité du trafic avec les réseaux des commerces extérieurs. S'il est excessif, le ralentissement conduit à l'expiration de la requête avant que celle-ci puisse parvenir à destination. Il s'apparente dans ce cas à un blocage ou à un filtrage par ralentissement de l'accès - on examinera plus loin les techniques de blocage et de filtrage.

Paragraphe 2 – La restriction du stockage de données

Deux techniques de restriction de l'accès dès le stockage de données seront tour à tour étudiées : le chiffrement et l'avertissement (A) ; puis la suppression de données (B).

A) Introduction à la restriction du stockage de données : les exemples du chiffrement et de l'avertissement

1. Le hachage, technique basique du chiffrement

On vient de voir que l'accès à une R-DATA peut être restreint au stade de la transmission de données. Dans ce cas, la restriction est pratiquée au niveau des moyens de transport (câbles terrestres et sous-marins, antennes hertziennes et bornes Wifi) et/ou des moyens d'acheminement (routeurs IP et passerelles). L'accès à une R-DATA peut aussi être restreint au stade du stockage de données. Dans ce cas, la restriction est pratiquée au niveau des moyens de stockage (serveurs, terminaux et périphériques accessoires).

564C'est ce que font certains opérateurs pratiquant du *zero rating*, privilégiant l'accès à certains services avec lesquelles ils sont engagés contractuellement au détriment des autres services dont l'accès est ralenti, v. « NGOs and academics warn against Deep Packet Inspection » [en ligne], sur *European Digital Rights (EDRi)*, mai 2019

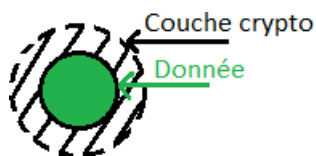
565C'est la manière dont procède la Chine pour empêcher l'accès à de nombreux réseaux ou services en ligne, v. WINTER Philipp et LINDSKOG Stefan, « How the Great Firewall of China is Blocking Tor » [en ligne], *USENIX -FOCI'12*, 2012

Moyens de transmission

Transport		Acheminement
Antennes et Borne Wi-Fi 	Câbles Terrestres 	Routeurs IP 
Câbles sous-marins 	Satellites 	

Moyens de stockage

Serveurs		Terminaux	Périphériques accessoires
Serveurs d'applications 	Serveurs DNS 	Ordinateurs 	Objets connectés 
Serveurs DHCP 	Serveurs de bases de données 	Smartphones 	Clés USB 
Serveurs de cache 	Serveurs de fichiers 	Tablettes 	Disques durs externes 
Serveurs de messagerie 	Serveurs de gestion 	Consoles de jeux 	Disques de stockage optique (CD-Rom, DVD-Rom, etc) 
...		TV connectées 	Cartes mémoires (y compris cartes SD) 



La donnée reçoit sa couche de protection de la part d'un algorithme de chiffrement. Par exemple, un logiciel de hachage fait correspondre un message (« Bonne fête maman ») à une valeur arbitraire et fixe (par ex. 00005f22d9c2a9ce84f6c8ca5d5943e3bbcb2d39758474c3d969c17359 e6cf212⁵⁶⁶). Chaque message ainsi chiffré reçoit une valeur H (ou « haché ») théoriquement unique, qui constitue l'« empreinte numérique » du message. De cette façon, la valeur H d'un message offre une couche de protection indissociable de ce message : le contenu de la donnée est occulté derrière sa valeur H. La couche de protection ne peut être levée qu'en résolvant le problème mathématique posé par l'algorithme de chiffrement. Par conséquent, pour lever la couche de

237

chiffrement et autoriser l'accès à la donnée chiffrée, l'algorithme doit fournir une formule de résolution – ou « clé » – du problème mathématique.

Le concepteur de l'algorithme de chiffrement peut choisir entre deux options. Soit il choisit une même formule de résolution (clé privée) pour chiffrer et déchiffrer les données – on parle alors de chiffrement symétrique. Soit le concepteur de l'algorithme choisit une formule pour chiffrer les données (en principe la clé publique) et une formule distincte pour déchiffrer les données (en principe la clé privée) – on parle alors de chiffrement asymétrique. Dès lors, quatre types d'algorithme de chiffrement sont classiquement reconnus⁵⁶⁷. Le chiffrement simple ou « chiffrement par substitution » consiste à remplacer les éléments d'un message par d'autres éléments, en recourant non pas à une clé de chiffrement ou de déchiffrement mais seulement à un code faisant correspondre les éléments substitués aux éléments de substitution (tel le chiffre de César qui fait correspondre $A \rightarrow X, B \rightarrow Y, C \rightarrow Z, D \rightarrow A, E \rightarrow B, F \rightarrow C \dots$). Cette méthode de chiffrement est facilement cassable. Le chiffrement par transposition consiste à faire permuter les éléments d'un même message (par ex., « sortie » devient « iorset »). Cette méthode est aussi aisément cassable, mais elle a le mérite d'avoir posé les bases du haché en proposant une liste aléatoire de caractères utilisables une seule fois (« masque jetable ») pour recouvrir le message clair. Ces deux méthodes de chiffrement, historiquement utilisées d'abord pour la communication militaire, ont été dépassées avec le développement des sciences mathématiques pour déchiffrer les messages et l'essor de la télégraphie qui aggrave le risque d'interception des messages par l'ennemi. À la fin du XIX^e siècle, le cryptologue militaire Auguste Kerckhoffs énonce six règles, rassemblées sous le nom de « principe de Kerckhoffs », qui précisent l'importance de posséder une clé de déchiffrement et servent encore aujourd'hui de référence en cryptologie⁵⁶⁸. Le concept de chiffrement à clé est, depuis, devenu cardinal en cryptologie numérique et a donné naissance aux deux autres méthodes de chiffrement qu'on a décrites : le chiffrement symétrique ou « à clé privé » (la même clé privée est utilisée pour le chiffrement et le déchiffrement) ; et le chiffrement asymétrique (une clé est utilisée pour le chiffrement, une autre pour le déchiffrement)

Lorsque la clé privée est stockée sur un serveur, le service qui fournit l'algorithme de chiffrement peut, depuis ses serveurs, déchiffrer toute donnée chiffrée à l'aide de son algorithme. On parlera dans ce cas de « chiffrement sur serveur ». Inversement, lorsque la clé privée est stockée sur le terminal de l'utilisateur, seul l'utilisateur peut, depuis son terminal, déchiffrer les données chiffrées à l'aide de cet algorithme. On parlera dans ce cas de « chiffrement sur terminal ». Dans le cadre d'une communication entre deux utilisateurs au

567EL MRABET Nadia, « Les concepts fondamentaux de la cryptographie » [en ligne], conférence à l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) de Rabat, Maroc, École des Mines de Saint-Étienne, semaine du 8 au 14 mars 2010

568Les règles de Kerckhoffs sont les suivantes : « 1. Le système doit être matériellement, sinon mathématiquement indéchiffrable ; / 2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ; / 3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ; / 4. Il faut qu'il soit applicable à la correspondance télégraphique ; / 5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ; / 6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer. », v. KERCKHOFFS Auguste, « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, janv. 1883, p. 5-38 (première partie) et KERCKHOFFS A., « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, fév. 1883, p. 161-191 (deuxième partie).

moins, le chiffrement asymétrique sur terminal est appelé « chiffrement de bout en bout ». Ainsi, les messageries instantanées Signal, WhatsApp, iMessage ou encore Rich Communication Service (messagerie SMS d'Android) pratiquent par défaut le chiffrement de bout-en-bout : chaque utilisateur possède sa propre clé privée (chiffrement sur terminal), de façon à pouvoir déchiffrer les messages qu'il reçoit sans que le service puisse déchiffrer et donc accéder aux messages échangés entre les utilisateurs ; et, distinctement de sa clé privée (chiffrement asymétrique), chaque utilisateur possède une clé publique grâce à laquelle il peut chiffrer ses messages et donc communiquer des messages chiffrés avec les autres utilisateurs.

Que la clé privée soit stockée sur un serveur ou sur un terminal, qu'il soit symétrique ou asymétrique, le chiffrement permet ainsi d'empêcher l'accès à une donnée par toute personne qui n'y est pas autorisée, *i.e.* par toute personne qui ne possède pas de clé privée délivrée par l'algorithme de chiffrement. Pour cette raison, le chiffrement a été instrumentalisé par plusieurs États pour restreindre l'accès à certaines R-DATA. C'est par exemple le cas des DRM (*Digital Rights Managements* ou « mesures techniques de protection »), techniques qui verrouillent l'accès à une œuvre protégée par un droit d'auteur. Les DRM procèdent en chiffrant un fichier qui comporte une œuvre protégée, pour ne rendre ce fichier lisible ou modifiable que par les logiciels ou les matériels détenant la clé de déchiffrement. On a vu la consécration des DRM par la directive européenne 91/250 de 1991, par les traités sur le droit d'auteur (WCT) et sur les interprétations et exécutions et les phonogrammes (WPPT) de 1996 de l'Organisation Mondiale de la Propriété Intellectuelle, et par le *Digital Millenium Copyright Act* de 1998 aux États-Unis. De même, en France, l'article L. 335-3-1 du Code de la propriété intellectuelle punit d'une amende de 3 750€ le fait de contourner, de neutraliser ou de supprimer intentionnellement un DRM, et d'une peine de six mois d'emprisonnement le fait pour une personne de proposer ou de procurer des outils qui portent atteinte à un DRM.

1. La signature électronique, technique authenticatrice du chiffrement

Outre les DRM, le chiffrement est aussi exploité par les États dans le cadre du dispositif de signature électronique. La signature électronique est un outil de chiffrement destiné à authentifier l'auteur d'un document informatique tout en préservant l'intégrité de ce document. Pour obtenir un tel résultat, la signature est produite en combinant l'une des clés du signataire (clé publique ou privée unique à ce signataire) avec l'empreinte numérique du message signé (valeur H unique à ce message), de telle sorte que $s_m = c(k, H(m))$ où s_m est la signature du message, k est la clé (publique ou privée) utilisée par le signataire, $H(m)$ est l'empreinte du message signé et c est la méthode de chiffrement appliquée à l'empreinte du message au moyen de la clé utilisée. Dès lors que la signature électronique est le résultat de cette équation, elle est solidaire de l'empreinte du message signé et de la clé utilisée : le message ne peut pas être altéré sans que la signature soit elle-même altérée, et la signature ne peut pas être altérée sans que le message soit lui-même altéré. Le plus souvent, la clé utilisée pour produire la signature électronique est la clé privée. Il en va ainsi de l'algorithme de chiffrement RSA (Rivest-Shamir-Adleman), qui propose la formule $s_m = c(k_{pr}, H(m))$ où k_{pr} est la clé privée du signataire⁵⁶⁹. De cette façon, seule la personne autorisée à déchiffrer la donnée (*i.e.* détenant la clé privée) est autorisée à la signer.

569GBÈTOHO SAHO Nelson Josas, EZIN C. Eugène, « Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm », *CARI 2020 - Colloque Africain sur la Recherche en Informatique et en Mathématiques Appliquées*, Oct 2020, Thiès,

Sur le plan juridique, la signature électronique sécurise triplement le contrat électronique (*i.e.* le contrat passé par voie informatique, comme les achats et les ventes en ligne) : le contrat signé électroniquement est authentique (chaque partie au contrat signe avec sa propre signature), intègre (le contenu du contrat ne peut pas être modifié entre le moment où il est signé et le moment où il est consulté ultérieurement) et non-répudiable (aucune des parties ne peut remettre en cause le contrat signé). Cependant, la signature électronique n'apporte une telle sécurité que si elle est efficace, c'est-à-dire si elle fait preuve d'une résistance aux collisions et aux attaques de préimage.

L'attaque de préimage survient lorsque l'attaquant ne connaît que $H(m)$ sans connaître le message m . À titre illustratif, supposons qu'un réseau social ne stocke les mots de passe des utilisateurs dans sa base de données que sous la forme de leurs empreintes numériques ; dès lors, un cyberattaquant qui accède à ladite base de données (par pénétration dans la base de données ou par fuite de données) accèdera non aux données {username,password} mais aux données {username, $H(\text{password})$ }. Il n'a donc pas accès aux mots de passe eux-mêmes (m), mais seulement à leurs hachés ($H(m)$). On appelle y la valeur H du mot de passe recherché, tel que $H(m) = y$ (en l'espèce, $H(\text{pseudonyme}) = y$). **L'attaque de pré-image consiste, en connaissance de $H(m)$, à tester un message m_2 de façon que $H(m_2) = y$.** En découvrant un message m_2 dont le haché est identique au haché du message m_1 , l'attaquant peut alors remplacer le message m_1 par le message m_2 sans que l'algorithme de chiffrement y voit une incohérence, et peut ainsi modifier les mots de passe malgré leur couche de chiffrement.

L'attaque de seconde préimage survient lorsque l'attaquant connaît à la fois $H(m)$ et m . Prenons l'exemple d'un document ministériel – tel qu'une circulaire publiée en ligne – portant la signature électronique du ministre concerné : un tel document est public de sorte que l'attaquant connaît le message m (en l'espèce, le contenu du document). Connaissant m , l'attaquant peut plus facilement remonter jusqu'à son haché à l'aide de calculs reprenant les éléments de l'équation de hachage (dont m)⁵⁷⁰. Il peut par ailleurs connaître le haché du document en pénétrant la base de données ou en profitant d'une fuite. **L'attaque de seconde préimage consiste ainsi, en connaissance de m et de $H(m)$, à tester un message m_2 de façon que $H(m_2) = y$,** où y correspond à la valeur H de la circulaire. En découvrant un message dont l'empreinte correspond à celle de la circulaire, l'attaquant peut alors manipuler le contenu du document pour le remplacer par m_2 , et signer la circulaire comme s'il en était le signataire originel.

Enfin, l'attaque par collision survient lorsque deux entrées différentes produisent le même haché. En effet, une fonction de hachage qui peut attribuer moins de sorties (*i.e.* de hachés) qu'il n'y a d'entrées (*i.e.* de messages) engendre nécessairement des collisions. L'attaquant peut profiter de cette faille de l'algorithme pour trouver deux messages m_1 et m_2 qui aboutissent à la même valeur H . Tandis que les attaques par préimage consistent à exploiter une seule entrée (m_2), **l'attaque par collision consiste à exploiter deux entrées m_1 et m_2 de façon que $H(m_1) =$**

Senegal. Les principaux dérivés de RSA sont RSASSA-PKCS-v1_5 (algorithme déterministe qui attribue une signature unique à l'utilisateur, valable pour tous ses messages) et, plus récemment, RSASSA-PSS (algorithme probabiliste qui, intégrant un facteur d'aléa dont dépend toute sortie, attribue une signature différente pour chaque message). *A contrario*, certains algorithmes de chiffrement comme les signatures Schnorr, ElGamal et le DSA (*Digital Signature Algorithm*) font résulter la signature de la clé publique.

⁵⁷⁰Par exemple, pour l'algorithme $H(m) = m^d \bmod p q$, où p et q sont deux grands nombres premiers et d est une constante publiquement accessible aux utilisateurs, l'attaquant peut retrouver le haché de m à l'aide de $m_2 = mpq + m$, auquel cas $H(mpq + m) = (mpq + m)^d \bmod p q = m^d \bmod p q$

H(m₂). Les explications qu'on a livrées ici sur les attaques de préimage et les collisions nous viennent de publications scientifiques spécialisées dans le domaine du chiffrement ⁵⁷¹. En revanche, les exemples précédemment proposés pour les attaques de préimage (mots de passe et document signé) nous viennent de la réponse d'un étudiant du Rochester Institute of Technology – Ross Snider désormais Ingénieur de sécurité chez Tesla d'après son compte LinkedIn – publiée sur StackExchange ⁵⁷². On a jugé ces illustrations pertinentes, et on reprendra ici l'exemple proposé par R. Snider pour l'attaque par collision :

« [L'attaquant] Bob trouve une collision entre deux binaires b et b' (c'est-à-dire que $H(b)=H(b')$) tels que b est un correctif de sécurité Microsoft Windows valide et que b' est un logiciel malveillant. Bob travaille pour Windows. Bob transmet son correctif de sécurité à la hiérarchie, (...) qui signe le code et envoie aux utilisateurs de Windows du monde entier le code binaire correspondant, dans le but de corriger une faille de sécurité. Bob peut maintenant contacter et infecter tous les ordinateurs Windows du monde avec b' et la signature que Microsoft a calculée pour b . »

La sécurité offerte par un algorithme de signature dépend alors de la facilité avec laquelle un attaquant peut trouver deux entrées dotées du même haché, en se servant d'une seule entrée (attaques de préimage) ou de deux entrées (attaque par collision). Plus l'algorithme limite la possibilité de trouver deux messages ayant un haché identique, plus il est résistant aux collisions et aux attaques par préimage. Cette différence entre algorithmes de signature sécurisés et non sécurisés a d'importantes conséquences pour la sécurité du contrat électronique : un contrat électronique signé par un algorithme non sécurisé, donc très susceptible d'être altéré, dépend-il du même régime juridique qu'un contrat électronique signé par un algorithme sécurisé ? Ces deux contrats ont-ils les mêmes effets juridiques ? Ont-ils la même valeur probatoire ?

Le législateur européen répond à ces questions en 2014, dans le cadre du règlement eIDAS (Electronic Identification Authentication and trust Services)⁵⁷³. Tout d'abord, ces deux contrats ne partagent pas le même régime juridique. Le règlement eIDAS échelonne plusieurs niveaux de sécurisation offerts par la signature électronique selon : leur degré de fiabilité ; et leur degré de complexité. Concernant les degrés de fiabilité d'un algorithme de signature, le règlement définit

571 Sur la résistance aux attaques de préimages et aux collisions, v. ROGAWAY Philip et SHRIMPTON Tom, « Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance », *Fast Software Encryption (FSE)*, vol. 3017, 2004, p. 371-388. Sur la différence mathématique entre les attaques de préimages et les collisions, Lars Knudsen et John Mathiassen les résument ainsi : l'attaque de préimage correspond au problème « considérant $y = H(x)$, trouver x' tel que $H(x') = y$ » (l'attaquant connaît seulement $H(x)$ et doit trouver un x' dont le haché a la même valeur que le haché de x) ; l'attaque de seconde préimage correspond au problème « considérant x et $y = H(x)$, trouver $x' \neq x$ tel que $H(x') = y$ » (l'attaquant connaît x et $H(x)$) ; l'attaque par collision correspond au problème « trouver x et x' tel que $x \neq x'$ et $H(x) = H(x')$ ». V. KNUDSEN Lars R. et MATHIASSEN John E., « Preimage and Collision Attacks on MD2 », *Fast Software Encryption (FSE)*, 2005, p. 255

572 « What is the difference between a second preimage attack and a collision attack? », sur *Stackexchange.com*, août 2010. StackExchange un réseau social de questions-réponses qu'on estime globalement fiable sur les questions techniques. Surtout, la réponse proposée par R. Snider nous semble tout à fait cohérente avec les publications scientifiques citées dans la dernière note.

573 Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

les degrés faible (« *degré limité de fiabilité* » pour identifier une personne), substantiel (« *degré substantiel de fiabilité* » pour identifier une personne) ou élevé (« *niveau de fiabilité plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel* »)⁵⁷⁴. Les États membres sont souverains pour reconnaître un algorithme de signature (ou « *schéma d'identification électronique* ») comme étant ou non sécurisé. Cependant, ils doivent notifier à la Commission européenne les algorithmes de signature qu'ils reconnaissent, en indiquant une description de l'algorithme et le degré de fiabilité que l'État lui reconnaît⁵⁷⁵. Les algorithmes reconnus par les États comme sécurisés doivent être interopérables, garantir le respect de la vie privée et des données à caractère personnel, et ne doivent pas discriminer d'autres techniques nationales d'identification électronique⁵⁷⁶. Pour faciliter l'interopérabilité des différents algorithmes de signature sur le territoire de l'UE, le règlement eIDAS impose une obligation de reconnaissance mutuelle. Concrètement, si un État membre exige l'utilisation d'un algorithme de signature spécifique pour accéder à un service en ligne fourni par un organisme du secteur public (telle la plateforme FranceConnect en France⁵⁷⁷), cet État doit reconnaître les algorithmes de signature utilisés par les autres États membres pour permettre aux résidents de ces derniers États d'accéder au service concerné⁵⁷⁸. Toutefois, si un algorithme de signature notifié par un État membre est altéré au point d'« *affecter la fiabilité de l'authentification transfrontalière* », cet État doit suspendre ou révoquer immédiatement ce moyen d'authentification ou ses éléments altérés⁵⁷⁹. L'authentification transfrontalière est ainsi préservée sur le territoire de l'UE, tout en limitant les risques d'insécurité que font courir certains algorithmes de signature et en laissant aux États membres le choix souverain des algorithmes de signature privilégiés sur le territoire national.

Concernant les degrés de complexité d'un algorithme de signature, le règlement en distingue trois : au plus bas niveau, se situe la simple signature électronique un ensemble de données « *jointes ou associées logiquement à d'autres données (...) et que le signataire utilise pour signer* » ; au niveau supérieur se situe la signature qualifiée, qui garantit l'authentification au moins du nom ou du pseudonyme de la personne physique signataire et qui est délivrée par un prestataire de confiance qualifié ; enfin, au niveau suprême se situe la signature avancée qui est liée au signataire de manière univoque, permet d'identifier le signataire, est placée sous le contrôle exclusif de ce dernier et rend détectable toute modification ultérieure des données signées⁵⁸⁰. Pour vérifier ces degrés de complexité, le règlement eIDAS s'appuie principalement sur des procédures de contrôle des prestataires fournissant un algorithme de signature. En vertu du règlement, les États doivent désigner un organe de contrôle (l'Anssi en France) chargé de distinguer les prestataires qui satisfont aux exigences du règlement et ceux qui n'y satisfont

⁵⁷⁴*Ibid.*, art. 8 et 9

⁵⁷⁵*Ibid.* art. 9

⁵⁷⁶*Ibid.*, art. 12

⁵⁷⁷ FranceConnect emploie effectivement un algorithme de signature : ALAUZEN Marie, « L'État plateforme et l'identification numérique des usagers », *Réseaux*, n° 212, 2019, p. 211-239

⁵⁷⁸Règlement eIDAS, art. 6. Cette obligation de reconnaissance ne s'applique que si trois conditions sont réunies : les algorithmes utilisés par les autres États membres doivent être notifiés à la Commission, proposer un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public, et présenter un niveau de garantie substantiel ou élevé.

⁵⁷⁹*Ibid.*, art. 10

⁵⁸⁰*Ibid.*, art. 3 et 26. Rien n'interdit à une signature avancée d'être par ailleurs qualifiée, i.e. d'être délivrée par un prestataire qualifié, v. art. 26§2

pas⁵⁸¹. Seuls les premiers se voient délivrer un certificat qualifié par l'organe de contrôle à leur propre demande⁵⁸². Qu'ils soient qualifiés ou non qualifiés, les prestataires doivent dans tous les cas : prendre les mesures techniques et organisationnelles adéquates pour garantir la sécurité du service fourni, notamment « *en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer [dans les meilleurs délais] les parties concernées des effets préjudiciables de tels incidents* » ; et notifier, dans un délai de moins de 24h après en avoir eu connaissance, à l'organe de contrôle (voire aux autres organismes concernés et aux organes de contrôle des autres États membres affectés) toute atteinte à la sécurité ou toute perte d'intégrité « *ayant une incidence importante sur le service de confiance ou sur les données à caractère personnel qui y sont conservées* »⁵⁸³. Les prestataires de confiance qualifiés subissent des mesures de contrôle supplémentaires : ils font l'objet, au moins chaque année, d'un audit effectué à leurs frais par un organisme évaluant la conformité au règlement eIDAS ; l'organe de contrôle peut à tout moment leur imposer un audit à leurs frais en plus de l'audit annuel, afin de confirmer que les prestataires qualifiés remplissent les exigences du règlement eIDAS ; et le prestataire qualifié doit corriger, dans le délai fixé par l'organe de contrôle, les manquements au règlement que l'organe de contrôle lui fait remarquer, sans quoi le prestataire pourra se voir retiré son certificat qualifié⁵⁸⁴. Les résultats des audits servent aussi la mission de coopération de l'organe de contrôle. En effet, l'organe de contrôle désigné par un État membre doit non seulement collaborer avec l'autorité nationale de protection des données personnelles (en lui faisant remonter les violations de données à caractère personnelles relevées à l'issue d'un audit) et les organismes et publics concernés par une atteinte à la sécurité ou une perte de données (en les informant de l'atteinte ou de la perte), mais aussi avec les organes de contrôle désignés par les autres États membres en leur prêtant assistance pour des demandes d'information ou d'inspection et en échangeant de « *bonnes pratiques* »⁵⁸⁵.

En instaurant des degrés de fiabilité de la signature électronique (faible, substantiel, élevé), et des degrés de complexité de la signature (signature simple, qualifiée, avancée), le règlement eIDAS hiérarchise les régimes juridiques de la signature selon le niveau de sécurité apporté⁵⁸⁶. Les signatures sécurisées et non sécurisées ne sont alors pas soumises au même régime juridique dans le droit de l'UE. Pour autant, le contrat signé par un algorithme non sécurisé a-t-il les mêmes effets juridiques que celui signé par un algorithme sécurisé ? Le règlement y répond par la négative : seuls la signature électronique qualifiée a un « *effet juridique (...) équivalent à celui d'une signature manuscrite* »⁵⁸⁷. Enfin, le contrat signé par un algorithme non sécurisé a-t-il la même valeur probatoire que celui signé par un algorithme sécurisé ? La réponse est cette fois positive : quel que soit le degré de fiabilité ou de complexité de la signature, « *l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent*

581Ibid., art. 17

582Ibid., art. 21. La demande doit inclure un rapport d'évaluation de la conformité au règlement délivré par un organisme d'évaluation de la conformité.

583Ibid., art. 19

584Ibid., art. 20

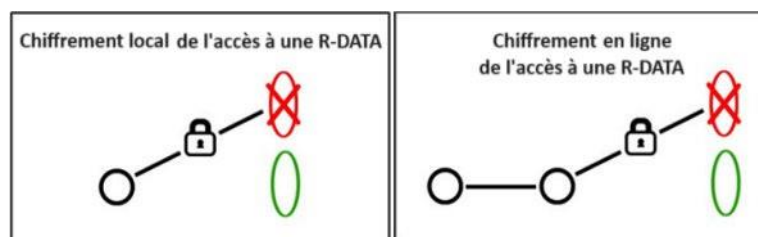
585Ibid., art. 17 et 18

586Par exemple, on a vu qu'un État membre ne peut reconnaître un algorithme de signature reconnu par un autre État membre que si cet algorithme présente un degré de fiabilité substantiel voire élevé, et supérieur ou égal à l'algorithme utilisé par le premier État. De même, la signature qualifiée est soumise à un régime nettement plus contraignant que la signature simple.

587Ibid., art. 25§2

être refusés au seul motif que cette signature se présente sous forme électronique ou qu'elle ne satisfait pas aux exigences de la signature qualifiée »⁵⁸⁸.

Pour réguler la signature électronique, le règlement eIDAS articule une coopération des États membres destinée garantir la sécurité, l'interopérabilité et l'homogénéité de la signature électronique sur le territoire de l'UE. En Corée du Nord, la signature électronique est exploitée pour empêcher l'accès des utilisateurs nord-coréens aux services étrangers. Depuis 2012, les systèmes d'exploitation des terminaux nord-coréens (Red Star OS pour les ordinateurs, généralement Android pour les smartphones) censurent l'installation de logiciels non certifiés par l'État. Pour ce faire, l'État appose sa signature électronique sur chaque logiciel qu'il certifie, et les systèmes d'exploitation des terminaux nord-coréens attribuent une signature électronique à chaque utilisateur. Lorsqu'un utilisateur nord-coréen (identifié comme tel par sa signature électronique) télécharge un logiciel non certifié par l'État, le système d'exploitation constate le défaut de signature étatique sur le logiciel non certifié et ne peut alors pas valider le téléchargement⁵⁸⁹. Le chiffrement et la signature électronique ont dans ce cas pour effet d'enfermer la Corée du Nord dans un environnement numérique strictement national. Il s'agit dans ce cas d'un chiffrement local, qui se produit sur le terminal de l'utilisateur, par opposition au chiffrement réseau qui se produit sur le serveur destinataire.



En somme, on reconnaît principalement deux avantages au chiffrement de données pour restreindre l'accès à une R-DATA. Premièrement, **le chiffrement sécurise l'accès à la donnée chiffrée** en faisant dépendre cet accès d'un problème mathématique complexe à résoudre. Concrètement, cela signifie qu'il est difficile de contourner la restriction d'accès à une donnée chiffrée si l'algorithme ne comporte pas de failles évidentes ou facilement exploitables. Par opposition, on verra que des techniques de restriction comme la suppression, le blocage ou le filtrage de données sont plus aisément contournables par les utilisateurs. Deuxièmement, en faisant dépendre d'un même algorithme de chiffrement un ensemble de données chiffrées, le chiffrement permet de **généraliser l'application d'une règle de nonaccès à chacune de ces données chiffrées par cet algorithme**. On appelle « règle de nonaccès » la règle par laquelle une donnée (la donnée inaccessible) ne peut pas être exécutée par une requête d'accès. Si la règle de nonaccès est posée par chiffrement, l'accès à ladite donnée est empêché soit parce que cette donnée est chiffrée, soit parce que la requête d'accès à cette donnée est chiffrée, soit parce que la donnée et la requête d'accès sont toutes deux chiffrées. L'algorithme de chiffrement a en ce sens un effet très centralisateur. En attribuant aux données chiffrées leur couche de protection,

⁵⁸⁸*Ibid.*, art. 25§1

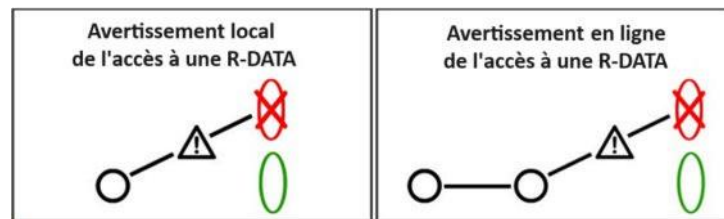
⁵⁸⁹GRUNOW Florian et SCHIESS Niklas, « Linfting the Fog on Red Star OS. A deep dive into the surveillance features of Nord Korea's operating system » (Conférence-Talk [en ligne]), *Chaos Computer Club*, 2015. Le Chaos Computer Club (CCC) est l'une des premières associations de hackers en Europe depuis les années 1980.

et en définissant le problème mathématique à résoudre pour lever cette protection, l'algorithme de chiffrement place sous son autorité toutes les couches protectrices des données qu'il chiffre, donc tout droit d'accès à ces données. De cette façon, aucune donnée chiffrée ne peut échapper à la règle de non-accès posée par son algorithme de chiffrement. On en a vu une illustration très extrême avec la signature électronique en Corée du Nord : une fois signées électroniquement, les requêtes produites par les Nord-Coréens ne peuvent plus accéder aux services en ligne non-agrérés par l'État, et il est très difficile de contourner ce mécanisme de signature électronique (cf. 1^{er} avantage du chiffrement).

Inversement, on reconnaît deux principaux inconvénients au chiffrement. Premièrement, **les avantages du chiffrement peuvent être exploités par les auteurs et les contributeurs de R-DATA**. Concrètement, les terroristes peuvent recourir au chiffrement pour sécuriser leurs échanges et organiser secrètement leurs attentats, les cyberattaquants peuvent y recourir pour contrôler l'ensemble des données constitutives de leur logiciel malveillant en y apposant une signature électronique unique (dans le cas d'un virus polymorphe par exemple), les utilisateurs peuvent se servir de VPN pour contourner le blocage ou le filtrage de données⁵⁹⁰ etc. Deuxièmement, chaque donnée chiffrée étant placée sous l'autorité de son algorithme de chiffrement, **les failles de l'algorithme de chiffrement valent pour toutes chacune des données chiffrées par cet algorithme**. Par conséquent, la connaissance par un attaquant des failles de l'algorithme de chiffrement lui fournit un contrôle sur chacune des données chiffrées par cet algorithme. Or, tout algorithme comporte nécessairement une faille. On en déduit que ce deuxième inconvénient du chiffrement peut être relativisé, certes en limitant le plus possible les failles exploitables, mais surtout en diversifiant le nombre d'algorithmes de chiffrement utilisés de manière à ce que les failles d'un seul algorithme ne permettent pas à l'attaquant de contrôler un nombre trop grand de données chiffrées.

590Un VPN (Virtual Private Network) est un réseau de serveurs, souvent éparpillés dans le monde, qui hébergent un logiciel qu'on appellera « application VPN ». Pour accéder à ce réseau de serveurs, l'utilisateur doit téléchargement localement, *i.e.* sur son terminal, le logiciel VPN correspondant appelé « client VPN » qui permet à l'utilisateur de communiquer avec l'application VPN hébergée sur les serveurs. Le client VPN chiffre localement les requêtes d'accès à internet émises par l'utilisateur, et ajoute dans le datagramme de ces requêtes l'adresse IP du serveur VPN destinataire choisi par l'utilisateur. Une fois que la requête est parvenue au serveur VPN destinataire, l'application VPN hébergée par ce serveur remplace l'adresse IP de l'utilisateur par celle du serveur VPN. Lorsqu'un utilisateur utilise un VPN, l'opérateur (Orange, Bouygues...) auquel est abonné l'utilisateur reçoit alors des données chiffrées depuis le terminal, puis les acheminent vers le serveur VPN, qui à son tour substitue l'adresse IP du terminal par l'adresse IP du serveur VPN. Une fois l'application VPN activée par l'utilisateur, les routeurs reçoivent donc des données chiffrées, et les services auxquels accèdent définitivement les utilisateurs (Google Search, YouTube, Facebook, Twitter...) reçoivent des données chiffrées et des adresses IP substituées. L'utilisateur du terminal peut soit emprunter un réseau VPN déjà déployé par un fournisseur VPN (ExpressVPN, Surfshark, NordVPN, Proton VPN...), soit louer des serveurs cloud auprès d'un fournisseur d'hébergement cloud (OVH, Scaleway, Microsoft Azure, Google Compute Engine, Digital Ocean...) et y héberger son propre service VPN à l'aide de logiciels de conception de VPN simples d'utilisation et en plein essor (OpenVPN, AlgoVPN...). Les VPN sont principalement utilisés pour la sécurisation des données professionnelles, le chiffrement de données personnelles ou encore le contournement de la censure ou de la surveillance.

2. L'avertissement



Outre le chiffrement, on relève une deuxième technique de restriction de l'accès à une R-DATA depuis le stockage de données : l'avertissement. On appelle « avertissement de l'accès à une R-DATA » la technique qui consiste à créer une étape qui informe l'utilisateur du risque d'accéder à une R-DATA. Par exemple, la directive européenne 2000/31 sur le commerce électronique prévoit la possibilité pour le consommateur d' « *identifier les erreurs commises dans la saisie des données et (...) de les corriger* » avant de finaliser une commande sur internet⁵⁹¹. Appelée « règle du double clic », cette disposition a été transposée en France par la LCEN de 2004 : le premier clic est exigé pour valider la commande, le second est exigé pour confirmer définitivement la commande après l'avoir vérifiée⁵⁹². La loi instaure ici une obligation d'avertissement, dans le but d'éviter au consommateur de passer une commande contraire à sa volonté.

Au-delà des transactions en ligne, la technique de l'avertissement est souvent employée contre les spams : les principales boîtes de messagerie (Gmail, Live, Yahoo! Mail, NetEase Mail...), la plupart des services de messagerie SMS et plusieurs réseaux sociaux (Instagram, Twitter...) rassemblent les spams détectés dans un espace dédié au spams. L'utilisateur peut les consulter, mais il est préalablement averti du risque que les messages rassemblés dans cet espace sont des messages indésirables. Un autre exemple très courant du recours à la technique d'avertissement est incarné par le message avertissant l'utilisateur que la page web à laquelle il souhaite accéder est non sécurisée. Cet avertissement est généralement mis en œuvre par le navigateur web (Chrome, Safari, Firefox, Edge, UC Browser...). Autre exemple : les systèmes d'exploitation et logiciels antivirus peuvent avertir l'utilisateur que le logiciel dont il requiert le téléchargement est suspect. Plus récemment, le projet de loi français visant à sécuriser et réguler l'espace numérique, présenté au Conseil des ministres le 10 mai 2023, envisage de créer une base de données répertoriant les sites frauduleux (infectés par des logiciels malveillants ou servant aux arnaques)⁵⁹³. Les opérateurs de transmission et/ou les navigateurs web devront apposer un avertissement sur les données figurant dans cette liste noire.

L'avertissement est aussi de plus en plus recouru contre les fausses informations : depuis 2017, Google Search associe un contexte aux résultats proposés par le moteur de recherche, qui permet à l'utilisateur de connaître la source de l'information et sa véracité potentielle, évaluée à partir des conclusions d'organisations tierces de vérification des faits (« *fact checking* ») comme

⁵⁹¹ Directive 2000/31/CE, art. 10, §1 c)

⁵⁹² Code Civil, art. 1127-2

⁵⁹³ Lettre de la DAJ – Projet de loi visant à sécuriser et réguler l'espace numérique, sur economie.gouv.fr, 10 mai 2023

Full Fact, Politifact et Snopes⁵⁹⁴. Cet outil de contextualisation sera plus tard appelé Google Fact Check Tools. Début 2021, Google Search ajoute une nouvelle fonctionnalité intitulée « à propos de ce résultat », qui fournit aux utilisateurs un résumé de Wikipédia relatif au résultat concerné⁵⁹⁵. Pour éviter les redondances entre ces deux outils contextuels, Google revoit entièrement sa fonction Google Fact Check Tools : en juin 2022, cet outil ne s'affiche plus aux côtés des résultats proposés par Google Search, mais fait l'objet d'un site web à part entière (toolbox.google.com)⁵⁹⁶. Ce site web est un moteur de recherche qui recense uniquement les vérifications de fausses informations effectuées par les vérificateurs d'information jugés crédibles. L'utilisateur qui doute de la véracité d'une information peut alors utiliser ce site web pour y rechercher ladite information (« terre plate », « vaccins Covid19 », « guerre Ukraine »...), et verra alors s'afficher une liste de résultats renvoyant vers des articles de fact checking traitant cette information. Chaque résultat proposé est décrit avec : l'affirmation qui fait l'objet de la vérification (« la terre est plate », « sur chaque vaccin Covid vendu 19,5 dollars, Pfizer fait plus de 18 dollars de marge », « Un « nuage radioactif » se dirige vers l'Europe de l'Ouest après l'explosion d'un « dépôt de munitions » »...); l'origine de cette affirmation (publications sur des réseaux sociaux, économiste interrogé par Complément d'enquête, autorités russes...); la source qui évalue la véracité de cette information (dpa-factchecking, TFI Info...); l'évaluation retenue par cette source (vrai, faux, partiellement vrai, trompeur...); et l'hyperlien renvoyant vers l'article vérifiant l'affirmation en cause.

On reconnaît deux principaux avantages à la technique de l'avertissement. Premièrement, les données dont l'accès fait l'objet d'un avertissement ne sont accessibles que sur décision de l'utilisateur. Les erreurs de modération ne se répercutent donc que moindrement sur l'accessibilité d'une donnée : si le modérateur humain ou le logiciel de modération appose par erreur un avertissement sur un site ou un contenu, ce site ou ce contenu demeurent accessibles à l'utilisateur qui décide de passer outre l'avertissement. Par conséquent, **les erreurs humaines ou logicielles de modération ont des conséquences très relatives sur l'accessibilité des données sanctionnées à tort car l'utilisateur peut toujours y accéder.** Deuxièmement, **l'avertissement est particulièrement adapté contre les données auxquelles les utilisateurs accèdent accidentellement.** On distingue en effet l'accès à des données selon que cet accès est intentionnel (publications de propos haineux, consultation de contenus pornographiques par des mineurs, harcèlement en ligne, téléchargements illicites d'œuvres protégées, consultation de contenus pédopornographiques...) ou non-intentionnel (spams, logiciels suspects, pages web malveillantes, arnaques...). On parle d'accès non intentionnel lorsque, une fois exécutées, les données stockées sont contraires à la volonté de l'utilisateur. En mettant en garde l'utilisateur, l'avertissement peut ainsi sérieusement le décourager d'accéder à des données présumées contraires à sa volonté.

Inversement, on voit deux principaux inconvénients à cette technique de restriction. Premièrement, **l'avertissement n'empêche pas l'utilisateur d'accéder à une R-DATA, mais**

⁵⁹⁴ TAN Corinne, « The curious case of regulating false news on Google », *Computer Law & Security Review*, vol. 46, sept. 2022

⁵⁹⁵ *Ibid.* Cette fonctionnalité prend la forme de l'icône « ⓘ », située à côté de chaque résultat. Par exemple, en cliquant sur l'icône associée aux résultats de la branche française du média russe d'État « Russia Today - France » (RT France), on lit le résumé Wikipédia : « *RT France, lancée en 2017 et interdite de diffusion en 2022 dans l'Union européenne, est la branche francophone de la chaîne internationale russe d'information en continu RT, créée en 2005 et financée par l'État russe.* [Hyperlien vers la page Wikipédia] »

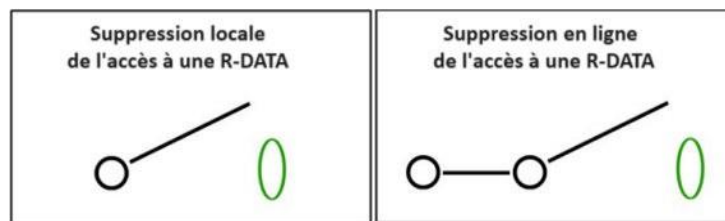
⁵⁹⁶ *Ibid.*

se limite à l'en décourager. L'efficacité de l'avertissement (i.e. la mesure dans laquelle il peut réduire l'échelle de diffusion d'une R-DATA) dépend donc de la force de conviction de cet avertissement. Deuxièmement, **l'avertissement est inadapté pour restreindre l'accès intentionnel à des données.** En effet, dès lors que l'accès aux données sanctionnées dépend de la décision de l'utilisateur, rien n'empêche l'utilisateur d'outrepasser l'avertissement pour accéder intentionnellement à ces données. Par conséquent, l'avertissement n'est adapté que pour limiter les accès accidentels à des données, mais se révèle inefficace contre les accès intentionnels.

B) La suppression de données

1. Les types de données supprimables : les exemples des comptes utilisateurs, des contenus et des fonctions logicielles

Comme le chiffrement et l'avertissement, la suppression de données est une autre technique de restriction spécifique au stockage de données. On appelle « suppression de données » la technique qui consiste à éliminer des données de l'espace mémoire qui les hébergeait. La suppression d'une R-DATA désigne l'élimination, depuis cet espace mémoire, de données refusées par le régulateur. La suppression de données peut être pratiquée localement (sur un terminal) ou en réseau (sur un serveur ou un périphérique accessoire).



On voit deux principaux avantages à la suppression de données. Premier avantage : **la suppression de données élimine l'existence même de ces données et donc leur accessibilité** depuis internet, puisque les données supprimées ne sont plus stockées par un espace mémoire informatique. Les données supprimées disparaissent ainsi du cyberspace tel qu'on l'a défini (ensemble des espaces mémoire interconnectés *via* internet). C'est, à notre connaissance, la seule technique de régulation d'internet qui présente un tel avantage. Son deuxième avantage découle du précédent : **la suppression de données est adaptée contre les R-DATA aussi bien intentionnelles qu'accidentelles.** En effet, à la différence de l'avertissement qui restreint surtout l'accès à des données potentiellement contraires à la volonté des utilisateurs (spams, logiciels suspects, pages web malveillantes, arnaques...), la suppression élimine les données de leur support de stockage et empêche donc tout utilisateur d'y accéder intentionnellement *et* accidentellement. Dès lors, la suppression est tout autant pertinente pour restreindre l'accès à des R-DATA intentionnelles (publications de propos haineux, consultation de contenus pornographiques par des mineurs, téléchargements illicites d'œuvres protégées, consultation de contenus pédopornographiques...) que pour restreindre l'accès à des R-DATA accidentelles.

On reconnaît en revanche deux inconvénients à la suppression des données. D'abord, **la suppression est une technique de régulation aisément contournable.** Il suffit pour cela de reproduire les données supprimées, ou de produire des données constitutives de la même illicéité que les données supprimées. Par exemple, si le régulateur fait supprimer dix fausses informations, les utilisateurs peuvent produire et diffuser dix autres fausses informations voire

reprendre exactement le contenu des fausses informations supprimées. Ensuite, **la suppression rend impossible d'individualiser l'accessibilité d'une donnée**. En effet, la suppression élimine des données d'un espace mémoire, donc ne permet plus à quiconque d'accéder à ces données. Inversement, d'autres méthodes comme le chiffrement, l'avertissement ou le blocage, qu'on étudiera plus loin, permettent restreindre l'accès d'une donnée à une ou plusieurs catégories de personnes. La suppression de données est donc moins adaptée que ces autres techniques pour limiter l'accès d'une donnée à certaines personnes. Par exemple, pour réserver aux majeurs la possibilité d'accéder aux contenus pornographiques, le blocage ou le chiffrement sont probablement plus pertinents que la suppression. Dans la mesure où la suppression élimine définitivement des données de l'espace mémoire sans permettre de trier les utilisateurs qui y ont ou non accès, cette technique doit être manipulée soigneusement et ne doit pas, en principe, être dirigée contre des données utiles à la majorité des utilisateurs (auquel cas de nombreux utilisateurs peuvent être tentés de contourner la suppression) ni contre des données importantes pour l'économie nationale (auquel cas la suppression définitive de ces données peut avoir de graves répercussions économiques). *A contrario*, le blocage, le chiffrement ou l'avertissement sont plus à même de réserver l'accessibilité de certaines données aux internautes qui en exploitent l'utilité.

La suppression de données est une technique classique pour restreindre l'accès à des contenus illicites. L'historicité et la popularité de cette technique s'expliquent probablement par son double avantage : la suppression provoque immédiatement un effet souvent recherché par le régulateur (à savoir la disparition de données illicites dans le cyberspace) et se montre adapté contre tout type d'accès aux données illicites par les utilisateurs (que les utilisateurs y accèdent intentionnellement ou non). La suppression de données peut être pratiquée manuellement – par un modérateur humain – ou bien automatiquement – par un logiciel de modération⁵⁹⁷. On examine ici trois types de données pouvant être supprimées : les données constitutives de contenus (texte, image, son, vidéo) ; les données constitutives d'un compte utilisateur ; et les données constitutives de fonctions logicielles.

● ***La suppression de contenus d'information et le bannissement par suppression***

Comme son nom l'indique, la suppression de contenus consiste à diriger la technique de suppression vers des contenus d'information stockés sur internet (textes, sons, images, vidéos). Elle peut être adaptée lorsque la R-DATA provient d'un contenu déterminé. On appelle « bannissement par suppression » la technique qui consiste à supprimer d'un service les données constitutives d'un compte utilisateur, de manière que ce compte et les contenus produits ou relayés par ce compte disparaissent de ce service. Cette technique peut être adaptée lorsque la R-DATA provient d'un utilisateur qui publie ou partage régulièrement des contenus illicites. Le bannissement par suppression empêche l'utilisateur de récupérer les données de son compte supprimé, contrairement au bannissement par blocage (comme la suspension de compte, *infra*) qui permet généralement à l'utilisateur bloqué de récupérer son compte une fois le blocage levé et aux autres utilisateurs d'accéder aux contenus du compte bloqué.

Dans la plupart des ordres juridiques étudiés, les hébergeurs et administrateurs de sites web ont en principe une liberté de moyens pour restreindre l'accès à des contenus illicites : ils peuvent supprimer les contenus illicites ou les comptes utilisateurs qui produisent ces contenus, ils peuvent bloquer l'accès à ces contenus ou à ces comptes, ils peuvent bloquer la diffusion de

⁵⁹⁷On étudiera plus loin les avantages et inconvénients des techniques de régulation manuelles par rapport aux techniques de régulation automatisées

publicités associées à un contenu illicite ou encore la capacité de l’auteur d’un contenu illicite à utiliser des moyens de paiement sur le service qui le sanctionne...

Quels que soient les moyens qu’ils mobilisent, ces acteurs sont tenus par une obligation de résultat – celle de limiter effectivement la présence d’un contenu ou d’un utilisateur sur son service en restreignant leur accessibilité ou leur survie économique. Du côté de l’UE, en présence d’informations illicites ou contraires aux conditions générales d’utilisation d’un service, le *Digital Services Act* (DSA) prévoit la possibilité pour l’hébergeur concerné « *de retirer des informations fournies par un [utilisateur] du service ou de rendre impossible l’accès à de telles informations, ou de restreindre d’une autre manière leur visibilité ou leur monétisation* »⁵⁹⁸. En revanche, lorsque l’hébergeur a effectivement pris connaissance de l’activité illégale ou du contenu illicite, il est obligé de « *retirer le contenu illicite [suppression] ou de rendre l’accès à celui-ci impossible [blocage]* »⁵⁹⁹. Le DSA de 2022 confirme ainsi la solution retenue par son ancêtre, la directive commerce électronique de 2000, et limite la responsabilité de l’hébergeur aux seuls contenus illicites dont il a effectivement connaissance qu’il n’a ni supprimés, ni bloqués. On a déjà relevé la liste des contenus illicites en France contre lesquels les hébergeurs et opérateurs doivent activement lutter⁶⁰⁰. Le DSA européen impose à tous les hébergeurs (sauf les micro ou petites entreprises) de publier un rapport annuel de transparence sur leur activité de modération⁶⁰¹, et ajoute l’obligation pour les « très grandes plateformes » (qui comptent 45 millions d’utilisateurs actifs par mois dans l’UE, soit 10% de la population européenne) de publier un rapport annuel évaluant les « *risques systématiques au sein de l’UE découlant de la conception ou du fonctionnement de leurs services* » et les mesures prises pour atténuer ces risques⁶⁰². Aux États-Unis, on a vu que les hébergeurs sont soumis au même régime de responsabilité, et on ne trouve aucune trace dans la législation fédérale qui orienterait les hébergeurs vers telle ou telle technique de restriction.

598Règlement 2022/2065 du 19 oct. 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE [ci-après « DSA »], cons. 54 et art. 17

599Ibid., art. 6

600Définie par l’art. 6, I, 7 LCEN et l’art. L336-2 du Code de propriété intellectuelle, cette liste cible : (i) la provocation à la commission d’actes de terrorisme, et l’apologie d’actes de terrorisme, de crime contre l’humanité, de crimes de guerre, de crimes de réduction en esclavage et de délits de collaboration avec l’ennemi ; (ii) les contenus pédopornographiques ; (iii) l’incitation à la haine raciale ; (iv) les contenus sexistes, homophobes, handiphobes et discriminants à raison de l’identité de genre ; (v) les contenus à caractère prostitutionnel, exposant la traite d’êtres humains, des violences sexistes ou des atteintes à la dignité humaine ; (vi) le harcèlement sexuel et le harcèlement scolaire commis sur internet ; (vii) et les atteintes au droit d’auteur

601DSA, art. 15 et 24. Le rapport de transparence doit mentionner : le nombre de demandes adressées par chaque autorité, classées selon le type de contenus illicites ; le temps de traitement ; le nombre de signalements d’utilisateurs classés selon le type de contenus et selon le type de fondement des réclamations (loi ou CGU) ; les types de mesures de modération initiées par l’hébergeur ; et le nombre de contestations dirigées contre les retraits des contenus et suspensions ou clôtures de comptes. V. sur le sujet l’analyse de REES Marc, « Le Digital Services Act expliqué ligne par ligne (articles 1 à 24) », *NextInPact*, 4 janv. 2021 et REES M., « Le Digital Services Act expliqué ligne par ligne (articles 25 à 74) », *NextInPact*, 6 janv. 2021

602DSA, art. 33 à 35

En Chine, la liste des contenus illicites est fixée dès 1997 – soit sept ans avant la France –, et n’a été que légèrement modifiée depuis⁶⁰³. En 2000, un décret du Conseil des affaires de l’État de Chine étend aux fournisseurs de contenus (« services d’information sur Internet ») l’obligation de faire respecter cette liste, qui contraignait jusqu’alors les seuls opérateurs de transmission de données⁶⁰⁴. Le régime de responsabilité contraste radicalement avec le régime occidental. D’une part, que l’hébergeur ait ou non connaissance des informations illicites qu’il diffuse, il engage sa responsabilité pénale si lesdites informations constituent une infraction pénale ; si lesdites informations ne constituent pas une infraction pénale mais représentent un risque pour la sécurité publique, l’hébergeur peut se voir imposer des avertissements, amendes, détentions administratives voire révocations des licences accordées⁶⁰⁵. D’autre part, si l’hébergeur a connaissance des informations illicites qu’il diffuse, il doit « *faire cesser immédiatement la diffusion de telles informations* » en étant libre de ses moyens pour atteindre cette fin⁶⁰⁶ ; si l’hébergeur n’arrête pas immédiatement la diffusion d’informations illicites après les avoir découvertes, il peut se voir adresser des exigences de « *corrections* » de la part de l’autorité administrative des télécommunications de la province, de la région autonome ou de la municipalité relevant du gouvernement central, et peut même se voir retirer sa licence « *lorsque les circonstances sont graves* »⁶⁰⁷. Cette obligation d’« *arrêt immédiat* de la diffusion » en cas de découverte de contenus illicites par le fournisseur de service en ligne est une spécificité chinoise par rapport à l’UE, aux États-Unis et à la Russie. Par crainte de voir leur responsabilité pénale engagée ou leur licence retirée, les fournisseurs de services en ligne qui exercent leur activité en Chine se sont très tôt engagés à pratiquer une autocensure draconienne et à détecter le plus rapidement possible les informations illicites partagées sur leur service⁶⁰⁸.

603Conseil des affaires de l’État, Règlement sur la sécurité de la République populaire de Chine, la protection et la gestion des réseaux d’information et d’Internet (计算机信息网络国际联网安全保护管理办法) du 30 déc. 1997, art. 5. Les contenus d’information interdits sont ceux qui : « (i) sont contraires aux principes fondamentaux énoncés dans la Constitution ; (ii) portent atteinte à la sécurité nationale, divulguent les secrets d’État, constituent une menace pour le gouvernement ou pour l’unité de la nation ; (iii) nuisent l’honneur et aux intérêts de l’État ; (iv) incitent à la haine ou à la discrimination ethniques ou nuisent à l’unité nationale ; (v) vont à l’encontre des politiques de l’État en matière de religion, ou qui contribuent à la promotion d’organisations hérétiques, de croyances féodales et de superstitions ; (vi) répandent des rumeurs qui perturbent l’ordre social ou menacent la stabilité sociale ; (vii) diffusent des informations à caractère pornographique ou licencieux, encouragent le jeu, la violence, l’homicide et la terreur, ou incitent à commettre des crimes ; (viii) propagent des informations insultantes ou diffamatoires, ou qui portent atteinte aux droits et intérêts légitimes d’autrui ; (ix) sont contraires à la loi ou aux règlements administratifs » (liste actuelle, telle que révisée par le décret n° 292 du Conseil des affaires de l’État de septembre 2000 pour y insérer la référence aux secrets d’État)

604Conseil des affaires de l’État de la République populaire de Chine, Décret n° 292 « Mesures relatives à l’administration des services d’information sur Internet » (互联网信息服务管理办法), 25 sept. 2000, art. 15

605Ibid., art. 20

606Ibid., art. 16

607Ibid., art. 23

608Par exemple, le réseau social de microblog Weibo (ressemblant à Twitter) se sert d’un logiciel pour scanner les messages des utilisateurs et identifier au plus tôt les contenus illicites pour pouvoir les supprimer : ZHANG Karen, « The promises and pitfalls of digital activism: Fighting for #MeToo

En Russie, cette stratégie juridique d'autocensure est consacrée depuis 2021, imposant toutefois une pression moindre que la Chine sur les fournisseurs de services en ligne. La loi sur l'autorégulation des réseaux sociaux de 2021 s'applique uniquement aux réseaux sociaux, définis très largement comme « *tout site web et/ou page web du site sur Internet, et/ou système d'information, et/ou logiciel utilisé ou destiné à être utilisé par ses clients pour fournir et/ou diffuser par le biais de leurs pages personnelles des informations dans la langue nationale de la Fédération de Russie, les langues nationales des républiques au sein de la Fédération de Russie et d'autres langues des peuples de la Fédération de Russie, sur lequel la publicité peut être distribuée afin d'attirer l'attention des consommateurs situés sur le territoire de la Fédération de Russie* »⁶⁰⁹. Les réseaux sociaux qui totalisent au moins 500 000 visiteurs quotidiens en Russie sont obligés d'empêcher que leur plateforme soit utilisée à des fins illicites (pour la commission d'infraction pénales, la divulgation d'informations constituant un secret d'État ou protégé par la loi, la diffusion d'appels publics à mener des activités terroristes ou les justifications publiques du terrorisme, la diffusion de contenus extrémistes, pornographiques, promouvant le culte de la violence et de la cruauté et la publication de textes obscènes), de prévenir la diffusion sur leur service de contenus diffamants et discriminatoires (à l'encontre d'un citoyen ou d'une catégorie de citoyens selon leur sexe, leur âge, leur race, leur appartenance ethnique, leur langue, leur attitude à l'égard de la religion, leur profession, leur lieu de résidence et de travail, ou leurs convictions politiques), de se conformer aux interdictions et restrictions posées par la législation fédérale russe sur le référendums et élections, et de respecter les droits et les intérêts légitimes des citoyens et des organisations (notamment leur honneur, dignité et réputation commerciale)⁶¹⁰. Cette autocensure active s'accompagne d'une obligation, pour les réseaux sociaux exerçant sur le sol russe et dont l'audience dépasse les 500 000 utilisateurs quotidiens, de surveiller activement la diffusion d'une vaste liste de contenus illicites⁶¹¹. Chaque « grand »

under the Great Firewall of China », *ANU Undergraduate Research Journal*, vol. 11, n° 1, avr. 2021. De même, depuis la fin des années 2010, le réseau social le plus utilisé en Chine WeChat analyse chaque message échangé sur sa plateforme dans le but d'améliorer la réactivité et la pertinence de ses algorithmes de censure : KNOCKEL Jeffrey, PARSONS Christopher, RUAN Lotus, XIONG Ruohan, CRANDALL Jedidiah et DEIBERT Ron, « We Chat, They Watch. How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus », sur *Citizenlab.ca*, 7 mai 2020

609 Loi fédérale n° 530-FZ du 30 décembre 2020 portant modification de la loi fédérale sur l'information, les technologies de l'information et la protection de l'information, art. 1^{er}, 1), 1, ajoutant un art. 10.6 à la loi sur l'information de 2006

⁶¹⁰ *Ibid.*, art. 1^{er}, 1), 1, §1 à §4

⁶¹¹ *Ibid.*, art. 1^{er}, 1), 1, §5. La liste des contenus à suivre activement est la suivante : (i) les contenus pédopornographiques ; (ii) les informations sur les méthodes de développement, de fabrication et d'utilisation de produits stupéfiants et autres substances psychoactives potentiellement dangereuses ; (iii) les informations sur les moyens de se suicider et les appels au suicide ; (iv) les informations qui organisent illégalement des jeux d'argent et des loteries sur internet ; (v) les informations qui permettent la vente à distance de boissons et de produits alcoolisés ; (vi) les informations qui sollicitent ou impliquent des mineurs dans la commission d'actes illégaux menaçant leur vie, leur santé ou celles d'autrui ; (vii) les expressions indécentes portant atteinte à la dignité humaine, à la moralité publique, aux symboles officiels de la Fédération de Russie, à sa Constitution ou aux organes exerçant le pouvoir d'État dans la Fédération ; (viii) les appels à des émeutes de masse, à la conduite d'activités extrémistes et à des événements de masse ne respectant pas la procédure légale, et la diffusion de fausses informations (« *informations socialement significatives non fiables diffusées sous l'apparence de messages fiables, qui menacent de porter atteinte à la vie et/ou à la santé des citoyens et/ou à leur propriété, menacent de perturber massivement l'ordre public et/ou la sécurité publique, ou menacent d'interférer avec le fonctionnement ou l'arrêt du fonctionnement des installations vitales, des infrastructures de transport ou sociales, des organismes de crédit, des installations énergétiques,*

réseau social doit conférer à ses utilisateurs le pouvoir de contester, au moyen d'un formulaire, les sanctions prises par le réseau social contre cet utilisateur ou ses contenus. Les grands réseaux sociaux doivent publier un rapport annuel exposant l'état des plaintes reçues et les résultats de la surveillance active des contenus⁶¹².

Tant dans l'UE qu'aux États-Unis, en Chine ou en Russie, les fournisseurs de services en ligne jouissent d'une liberté de moyens, dont la suppression de contenus et le bannissement d'utilisateurs⁶¹³. Cette liberté de moyens est le terreau légal sur lequel peuvent être expérimentées diverses stratégies de régulation puis évalués leurs résultats. Les différences entre ces ordres juridiques résident principalement dans le régime de responsabilité des fournisseurs de services en ligne et dans la liste des contenus illicites.

● *La désactivation de fonctions par suppression*

Les contenus et les comptes utilisateurs ne sont évidemment pas les seules données pouvant être sanctionnées. Les fonctions logicielles aussi peuvent être désactivées. On s'attarde ici sur la technique qui consiste à désactiver une fonction logicielle en supprimant les données qui la constituent⁶¹⁴. Désactiver une fonction a pour effet de priver l'utilisateur de la capacité d'action que lui offrait cette fonction. La désactivation d'une fonction est alors adaptée contre une R-DATA qui provient d'une capacité d'action précise. Inversement, si la R-DATA peut provenir d'une multitude de capacités d'action, les utilisateurs pourront toujours exercer des capacités d'action non désactivées pour diffuser cette R-DATA, et la désactivation d'une seule de ces capacités sera donc moindrement voire aucunement efficace contre cette R-DATA.

On prend pour exemple l'ancien onglet « Activité » sur Instagram. Jusqu'en 2019, cet onglet était la fonction d'utilisation par défaut du réseau social. Il proposait sur la page d'accueil de l'utilisateur un fil d'actualité retraçant l'activité des autres membres du réseau social suivis par cet utilisateur (les contenus qu'ont aimés et créés les membres suivis, les nouvelles relations des membres suivis, leurs changements de statut...). Jugeant que cette fonction favorisait le cyberharcèlement à travers le « stalking » (i.e. le fait, pour un harceleur, de surveiller ses victimes), Instagram l'a supprimée en octobre 2019. Or, le stalking et le harcèlement en ligne peuvent s'exercer grâce à de nombreuses autres fonctions que l'onglet Activité, notamment les fonctions de messagerie

industrielles ou de communication ») ; (ix) la diffusion d'informations par une ONG reconnue comme « indésirable » sur le territoire fédéral russe ; (x) et toute information sur la manière d'accéder à l'une des informations précitées (tel que les logiciels pour contourner les restrictions ou encore les contenus décrivant des moyens de contournement)

⁶¹² *Ibid.* art. 1^{er}, 1), 1, §7

⁶¹³ Par exemple, d'après son rapport de transparence de septembre 2022, TikTok a supprimé 113 millions de vidéos entre avril et juin 2022, soit environ 0,95% de la totalité des vidéos publiées sur TikTok durant cette période ; ce taux de suppression est en très légère baisse par rapport à avril-juin 2022 (1%) et en légère hausse depuis juillet-septembre 2020 (0,7%) : « Community Guidelines Enforcement Report Apr-Jun 2022 », sur *TikTok.com*, 28 sept. 2022 ; SATO Mia, « TikTok removed 113 million videos in three months », *TheVerge*, 28 sept. 2022. De même, entre octobre et décembre 2022, YouTube a supprimé près de 6,5 millions de chaînes (bannissement d'utilisateurs par suppression de leur chaîne) et 5,6 millions de vidéos (suppression de contenus) : « YouTube Community Guidelines enforcement », sur *Transparencyreport.google.com*, consulté le 19 mai 2023. Entre janvier et mars 2022, Facebook a supprimé près de 45 millions de contenus attentatoires aux droits d'auteur, et a restreint près de 90 000 autres contenus illicites ou contraires à ses CGU : « Transparency Report, First Half 2022 », sur *About.fb.com*, nov. 2022

⁶¹⁴ On verra plus loin qu'elles peuvent être désactivées par blocage

privée, de visites des profils, de partage de vidéos et de publication de commentaires, dont certaines sont des fonctions essentielles à l'utilisation du service (notamment la messagerie privée et les visites de profil). La désactivation de cet onglet a donc été inefficace pour lutter contre le cyberharcèlement sur Instagram : 20% des enfants de moins de 18 ans étaient victimes de cyberharcèlement sur Instagram en 2017, contre 30% en 2022, soit une forte hausse malgré la désactivation de sa fonction par Instagram⁶¹⁵. Par conséquent, **la désactivation d'une fonction n'est adaptée que lorsqu'une R-DATA provient principalement de la capacité d'action désactivée.**

2. Méthode de suppression de données : l'exemple du déréférencement

Le déréférencement consiste, pour un moteur de recherche, à retirer de sa liste de résultats ceux qui renvoient vers une R-DATA (site web à caractère terroriste ou infecté par un logiciel malveillant, page web contenant des propos haineux, diffamatoires, violant un droit d'auteur ou le droit d'autrui à une vie privée, hyperliens renvoyant vers des marchandises pédopornographiques ou des produits stupéfiants...). À ce jour, on identifie principalement trois autorités capables d'obliger juridiquement un moteur de recherche à déréférencer ses résultats.

Premièrement, l'ordre de déréférencement peut provenir de l'autorité judiciaire. En France, cette possibilité a été consacrée pour la première fois dans la décision *Allostreaming* de 2013. En l'espèce, les ayants-droits se fondaient sur l'article L336-2 du Code de la propriété intellectuelle pour porter deux demandes devant le juge judiciaire⁶¹⁶. Ils lui réclamaient d'abord d'ordonner à Google Search ce qu'on appellera un « déréférencement fixe » des sites litigieux, *i.e.* le déréférencement d'une liste déterminée de résultats litigieux (en l'espèce, des sites de streaming illégal). Ils lui réclamaient ensuite d'ordonner à Google Search de déréférencer toutes les pages web donnant accès à ces sites. On parlera dans ce cas de « déréférencement extensif », *i.e.* le déréférencement de résultats jugés équivalents aux résultats figurant sur la liste de déréférencement fixe. Le juge satisfait à leur première demande mais pas à la seconde, au motif que, « *en l'état de la législation applicable* », il ne disposait pas de la capacité matérielle pour contrôler l'exécution d'une telle décision⁶¹⁷.

Bien que l'état de la législation n'ait pas changé sur ce point, le juge judiciaire français adopte une toute nouvelle position en 2017. D'abord, il estime qu'un déréférencement fixe est insuffisant pour protéger le droit d'auteur : « *il n'y a pas lieu (...) de cantonner les mesures de déréférencement sollicitées aux seules pages ciblées des sites litigieux (...) alors que (...) un même site ou un même nom de domaine peut contenir des milliers de pages et autant d'adresses URL différentes, et que le nombre et le contenu de ces pages peuvent évoluer à tout moment* »⁶¹⁸. Par conséquent, poursuit le juge, un déréférencement fixe qui obligerait les ayants-droits à redéfinir constamment la liste de chaque URL à déréférencer « *serait totalement inefficace (...) puisque ces mesures seraient aisément contournables dès lors que les sites*

⁶¹⁵« The Annual Bullying Survey 2017 », sur *Ditchthelabel.org* [organisme caritatif international d'aide aux jeunes], juil. 2017 ; « Cyberbullying in Plain Sight. A McAfee Connected Family Report », *McAfee.com*, août 2022

⁶¹⁶L'art. L336-2 CPI autorise le juge judiciaire à prendre « *toute mesure* », à la demande des ayants-droits, à l'encontre des opérateurs de transmission et des hébergeurs pour restreindre l'accès à une atteinte à un droit d'auteur sur internet

⁶¹⁷TGI Paris, réf., *Allostreaming*, 28 nov. 2013 ; confirmé par CA Paris, 1^{ère} ch. Pôle 5, *Allostreaming*, 15 mars 2016, n° 040/2016 puis par C. Cass., *Allostreaming*, 6 juil. 2017, n° 16-17.217

⁶¹⁸TGI Paris, 3^e ch. 2^e sect., *Zone Téléchargement et autres*, 15 déc. 2017, n° 17/13471

litigieux créent en continu de nouvelles pages représentant autant de possibilités d'accès à l'intégralité de ces sites, (...) [et] indexées au fur et à mesure par le moteur de recherche ». Ce raisonnement conduit le juge à inclure le déréférencement extensif parmi son éventail de mesures contre les violations d'un droit d'auteur. Dès lors, le juge n'ordonne pas seulement à Google Inc. (désormais Alphabet Inc.) d' « *empêcher l'apparition [sur son moteur de recherche] de tout résultat en réponse à une requête émanant d'internautes à partir du territoire français (...) portant sur les sites [litigieux]* » listés par les ayants-droits et par la décision de justice (déréférencement fixe). Il lui ordonne aussi d'empêcher l'apparition, sur le territoire français, de tout résultat, non mentionné dans la liste des ayants-droits et de la décision de justice, « *renvoyant notamment vers l'une quelconque des pages des sites accessibles via les noms de domaine [litigieux]* »⁶¹⁹. En d'autres termes, Google Inc. est obligée de censurer sur le territoire français non seulement les sites listés par les ayants-droits et le juge, mais aussi les sites de redirection (adresses URL exclusivement dédiées au renvoi des requêtes vers les noms de domaines litigieux) non détectés par les ayants-droits et le juge ou susceptibles de naître après la décision de justice.

La décision de 2017 acte donc d'abord un dépassement du déréférencement fixe, tenu pour insuffisant face à la dynamique des résultats référencés par un moteur de recherche. Ensuite, autre évolution importante par rapport à l'arrêt *Allostreaming* de 2017, le dépassement du déréférencement fixe s'accompagne logiquement d'un dépassement du référencement par noms de domaines. En effet, les noms de domaines référencés par un moteur de recherche et employés par l'administrateur d'un même site web sont très changeants. Dès lors, « *il n'y a pas lieu non plus (...) de cantonner les mesures susceptibles d'être prises par la société [Google Inc.] aux seuls noms de domaine ciblés au jour de la demande et qui permettent, à cette date, l'accès aux sites litigieux* ». Dans ce cadre, le tribunal exige à Google Inc. d'empêcher l'accès aux sites litigieux, à partir non seulement de leurs noms de domaines (zonetelechargement.su, zone-telechargement.ru, papystreaming-hd.org, papy-streaming.org...) mais surtout des mots clés entrés par l'utilisateur (les mots clés « Zone Téléchargement », « Papystreaming » et « Sokrostream »)⁶²⁰. En d'autres termes, le déréférencement extensif (des sites de redirection) promu par le juge en 2017 repose sur des mots-clés davantage que sur des noms de domaine. Pour appliquer cette censure extensive au-delà des noms de domaine listés par le juge, ce dernier propose à Google Inc. : de rechercher, dans son index, les résultats qui exploitent une redirection 301 à destination de Zone Téléchargement, Sokrostream ou Papystreaming⁶²¹ ; ou encore de s'appuyer sur la Google Search Console (un outil exploité par les administrateurs de sites web pour suivre et améliorer leur référencement par Google Search) afin de suivre l'activité des administrateurs des sites litigieux.

Enfin, l'arrêt de 2017 ne limite plus les « *mesures devant être prises par un moteur de recherche* » au déréférencement. Le juge laisse à Google le choix entre deux options pour empêcher l'accès aux résultats litigieux depuis le territoire français : le moteur de recherche peut classiquement *déréférencer* les résultats litigieux et leurs sites de redirection, auquel cas il

619En l'espèce, les noms de domaine litigieux étaient les suivants : zonetelechargement.su, zone-telechargement.ru, zone-telechargement.eu, zone-telechargement.ws, papystreaming-hd.org, papy-streaming.org, papystreaming.org, sokrostream.ws, sokrostream.cc, sokrostream.biz et sokrostream.com

620Le tribunal impose ainsi à Google Inc. « *de procéder aux déréférencements des sites accessibles via les mots clés précisés dans la présente décision* »

621Une redirection 301 (ou HTTP 301 Moved Permanently) est un code de réponse interopérable avec le protocole Web (HTTP), qui permet de rediriger de manière permanente le trafic depuis une adresse URL vers une autre adresse URL

supprime les données de son index français (sur [google.fr](https://www.google.fr)) ; et/ou il peut *bloquer* l'accès des utilisateurs résidents en France aux résultats litigieux et à leurs sites de redirection, auquel cas il ne supprime pas les données de son index mais instaure une barrière qui prive ces utilisateurs d'accéder à ces données⁶²². En somme, l'arrêt *Zone-Téléchargement e. a.* de 2017 introduit, par rapport à l'arrêt *Allostreaming* de 2013, un changement de paradigme considérable pour la censure des atteintes au droit d'auteur en ligne. **Le paradigme du déréférencement fixe par noms de domaine (2013) est devenu celui d'une censure extensive par mots clés pouvant procéder d'un déréférencement et/ou d'un blocage (2017).**

Ce changement de paradigme est confirmé par le même tribunal le 25 mai 2018⁶²³. Le 13 juillet 2018, le juge considère pour la première fois que les ayants-droits peuvent agir en référé dans le cadre de l'art. L336-2 CPI⁶²⁴. Un tel apport accélère notablement le traitement par le juge judiciaire des demandes des ayants-droits pour restreindre l'accès aux violations de droits d'auteur en ligne. En décembre 2018, la même juridiction confirme, à l'encontre de sites diffusant des atteintes au droit d'auteur, la censure extensive par mots clés procédant d'un déréférencement et/ou d'un blocage à l'encontre des violations de droits d'auteur, précisant que Google doit s'appliquer à rechercher « *les nouveaux chemins d'accès* » aux sites censurés⁶²⁵.

Deuxièmement, outre l'autorité judiciaire, l'ordre de déréférencement peut provenir de l'autorité administrative. En France, cette possibilité est consacrée pour la première fois par une loi de 2020 qui autorise la Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF) à obliger les opérateurs de plateformes, « *en leur notifiant les adresses [URL] dont les contenus sont manifestement [contraires au droit de la consommation], de prendre toute mesure utile destinée à faire cesser leur référencement* » pour une durée arrêtée par l'autorité administrative (en principe le ministère de l'Économie)⁶²⁶. L'option

622À cette fin, Google peut par exemple déployer un blocage par géolocalisation (reposant sur la géolocalisation des appareils se connectant à Google Search, toutefois aisément contournable à l'aide d'un VPN notamment) ou encore un blocage par association des utilisateurs de Google Search avec leurs comptes Google Workspace (Gmail, Google Drive, Google Agenda...). Dans la décision judiciaire ici étudiée, rien n'interdit à Google Inc. de combiner déréférencement (suppression des données sur l'index [google.fr](https://www.google.fr)) et blocage (inaccessibilité pour les résidents en France des résultats litigieux sur les autres index de Google comme [google.com](https://www.google.com)).

623TGI Paris, 3^e ch. 2^e sect., *Filmstreamvk e. a.*, 25 mai 2018, n° 18/03028. Saisi par les mêmes requérants pour mettre à jour la liste des sites à censurer, le juge réitère l'obligation de Google Inc. d'« *empêcher l'apparition sur [Google Search] de tout résultat en réponse à une requête émanant d'internautes à partir du territoire français (...) renvoyant vers l'une des pages des sites "Filmstreamvk", "Filmzenstream", "K-streaming", "Papstream", "Serie-vostfr" et "Skstream" notamment accessibles via les noms de domaines "filmstreamvk.me", "filmstreamvk.co" [etc.]* »

624TGI Paris, réf., *FNDF e. a. c/ Orange e. a.*, 13 juillet 2018, n° 18/55236: l'article L336-2 « *n'exclut (...) pas explicitement la compétence du juge des référés, qui lui-même est une émanation du tribunal et dont le président, conformément à l'article L. 213-2 du code de l'organisation judiciaire, a compétence pour statuer en référé "en toutes matières"* »

625TGI Paris, 3^e ch. 2^e sect., *FNDF e. a. c/ Google Inc., Bouygues Telecom e. a.*, 14 déc. 2018, n° RG 18/10652

626Loi n° 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière, art. 5 insérant l'art. L.521-3-1 du Code de la consommation. Le déréférencement peut être ordonné par les agents habilités de la DGCCRF notamment contre les infractions suivantes : pratiques commerciales déloyales (agressives ou trompeuses) ; abus de faiblesse ; ventes ou prestations de services « à la boule de neige » (ventes

ici choisie est celle d'un déréférencement fixe : les hyperliens déréférencés sont ceux listés et définis par l'autorité administrative. Ce pouvoir de police administrative reconnu en 2020 a été exercé dès 2021. Après avoir ouvert une enquête sur la place de marché Wish en septembre 2020, la DGCCRF en a conclu en juillet 2021 que 90% des appareils électroniques, 62% des bijoux fantaisistes et 45% des jouets analysés par la DGCCRF et vendus su Wish étaient dangereux. La DGCCRF accuse Wish de tromper ses consommateurs et enjoint à la place de marché de se mettre aux normes dans un délai de deux mois, mais Wish ignore l'injonction. Conformément à la loi de 2020, la DGCCRF ordonne à Google Search en novembre 2021 de déréférencer les résultats renvoyant vers Wish pour une durée de 15 mois⁶²⁷.

Outre le déréférencement fixe, la loi française inclut aussi le déréférencement extensif depuis 2021. La loi contre le séparatisme confie à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) le pouvoir d'ordonner le déréférencement de tout service en ligne qui reprend « *en totalité ou de manière substantielle* » le contenu d'un service dont l'accès est déjà restreint par une décision judiciaire

consistant à faire espérer au consommateur l'obtention d'une marchandise ou de gains en subordonnant ces gains ou marchandises au placement de bons ou de tickets à des tiers ou à la progression du nombre d'adhérents ou d'inscrits plutôt qu'à la vente, la fourniture ou la consommation de biens ou services) ; les frais de recouvrement perçus ou sollicités par un professionnel auprès d'un consommateur ; les publicités non autorisées sur des opérations commerciales réglementées (toute publicité doit obtenir une autorisation pour certaines opérations commerciales comme les opérations de dégagement ou de catégories de produits alimentaires hors fruits et légumes frais, les publicités pour les ventes et rachats de marchandises effectués dans des lieux non destinés à la vente au public ou au rachat de ces marchandises...) ; le fait pour un professionnel, pour des motifs liés au lieu de résidence d'un consommateur, d'empêcher ce consommateur d'accéder à son interface en ligne, de le rediriger vers une version différente de celle à laquelle il a voulu accéder, de lui appliquer des conditions différentes de paiement, de vente ou de fourniture ; les publicités comparatives trompeuses, mettant en regard des biens ou services répondant à des besoins ou des objectifs différents, manquant de comparer ces biens et services selon leurs caractéristiques essentielles, pertinentes, vérifiables ou représentatives, dénigrant la concurrence, tirant indûment profit de la notoriété d'une marque, créant une confusion pour le consommateur entre les biens, services et signes distincts de l'annonceur et ceux d'un concurrent ; les publicités, offres promotionnelles (rabais, primes, cadeaux), concours et jeux promotionnels adressés par courrier électronique qui ne s'identifient pas clairement comme tels auprès du destinataire du courrier ou qui, proposés par voie électronique, ne précisent pas clairement ou ne rendent pas aisément accessibles les conditions pour bénéficier d'offres promotionnelles ; la vente d'échantillons ou la publicité en faveur des denrées alimentaires destinées aux enfants de moins de 4 mois ; les contrats qui ne sont pas présentés et rédigés de manière claire et compréhensible, qui n'indiquent pas la nature de l'avantage procuré par le consommateur (outre le prix), qui ne mentionnent pas les garanties légales des vices cachés et de conformité pour les biens, contenus et services numériques, qui contiennent des clauses abusives, ou qui ne sont pas conservés par le contractant professionnel si le contrat porte sur une somme égale ou supérieure à un montant fixé par décret (120€) ; les contrats de vente ou de fourniture de biens, de services ou de contenus numériques qui ne précisent pas l'application d'un prix personnalisé sur la base d'une prise de décision automatisé s'il y a lieu, ni les informations légales (caractéristique du bien, service ou contenu numérique, prix du bien, service ou contenu, date ou délai de livraison, identité, coordonnées postales, téléphoniques et électroniques du professionnel, activité de prestation de services du professionnel, modalités de résiliation, modes de règlement des litiges, possibilité de recourir à un médiateur, droit de rétractation lorsqu'il existe, charge pesant sur les consommateurs des frais de renvoi du bien en cas de rétractation, circonstances dans lesquels le consommateur peut exercer son droit de rétractation)...

627« Protection des consommateurs : lourde sanction pour la place de marché en ligne Wish », sur *Economie.gouv.fr*, 24 nov. 2021

pour avoir diffusé des contenus illicites tels que définis par l'art. 6, I, 7 LCEN⁶²⁸. On a vu que les atteintes au droit d'auteur justifient en principe un déréférencement extensif des sites de redirection par le juge judiciaire depuis 2017 ; depuis 2021, les contenus illicites énoncés par l'art. 6, I, 7 LCEN justifient en principe un déréférencement extensif des sites miroirs (copies exactes d'un site web) par l'autorité administrative.

Troisièmement, l'ordre de déréférencement peut provenir de l'utilisateur. L'internaute se sert dans ce cas son droit au déréférencement. Tel que consacré par la CJUE en 2014 dans son arrêt *Google Spain*, ce droit confère à l'utilisateur le pouvoir d'exiger d'un moteur de recherche qu'il retire de la liste de ses résultats, « *affichée à la suite d'une recherche effectuée à partir de [son] nom* », ceux d'entre eux « *publiés par des tiers et contenant des informations relatives à cette personne* »⁶²⁹. Fin mai 2014, soit moins de deux semaines après la jurisprudence *Google Spain*, Google Inc. met à disposition de ses utilisateurs européens un formulaire de demande de déréférencement⁶³⁰. Pour réclamer à Google le déréférencement des adresses URL qui comportent des données personnelles sur un utilisateur européen et qui s'affichent lors d'une recherche portant sur le nom et le prénom de cet utilisateur, il suffit alors à l'utilisateur concerné de remplir le formulaire en y joignant une pièce d'identité et les adresses URL litigieuses.

Pour autant, ce droit subjectif au déréférencement n'est pas absolu. D'une part, il est limité par la liberté d'information : si l'adresse URL dont le déréférencement est demandé concerne une page web qui comporte notamment des informations d'intérêt général, utiles au débat public ou relevant du droit d'archivage, le déréférencement de cette page peut être jugé contraire à la liberté des internautes de s'informer. Le moteur de recherche et le juge doivent alors effectuer une mise en balance entre le droit au respect de la vie privée du demandeur et la liberté d'information des autres utilisateurs pour ordonner un déréférencement de données personnelles⁶³¹. En 2022, la CJUE a toutefois précisé un cas systématique de déréférencement. Lorsque le résultat dont le déréférencement est demandé renvoie vers des informations « *manifestement inexactes* », la liberté d'information ne se heurte plus au déréférencement de telles informations. Dans ce cas, le moteur de recherche est donc « *tenu de faire droit à la demande de déréférencement* » sans l'intervention préalable d'une décision de justice – à charge pour le demandeur du déréférencement de prouver l'inexactitude manifeste⁶³². Le moteur de recherche est donc « *tenu de faire droit à la demande de déréférencement* » sans

628Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, art. 39 insérant un art. 6-3 à la LCEN

629CJUE, *Google Spain et Google Inc. c/ AEPD*, 13 mai 2014, n° 131/12, 3) du dispositif de l'arrêt

⁶³⁰ DELIGIA Florent, « Comment se faire oublier par Google : un formulaire en ligne », *Lyon Capitale* [en ligne], 30 mai 2014

631L'art. 17, §3, a) du RGPD de 2016 dispose que le droit à l'effacement de données à caractères personnelles par un responsable de traitement ne s'applique pas « *dans la mesure où ce traitement est nécessaire : a) à l'exercice du droit la liberté d'expression et d'information* ». À ce titre, l'exploitant du moteur de recherche doit « *vérifier* » que le résultat litigieux est « *nécessaire à la liberté d'information* », auquel cas cet exploitant n'est pas tenu de déréférencer ce résultat : CJUE, *GC e. a. c/ CNIL*, 24 sept. 2019, n° C-136/17, §56-66. Quant au juge saisi d'une telle demande de droit à l'effacement, il doit dépasser l'appréciation de la seule « *nécessité* » du résultat litigieux à la liberté d'information, pour effectuer une mise en balance plus subtile et approfondie entre, d'une part, le droit au respect de la vie privée et à la protection des données à caractères personnelles et, d'autre part, le droit à la liberté d'information : CJUE, *Google LLC c/ CNIL*, 24 sept. 2019, n° C-507/17, §67 et 72

632CJUE, *TU, RE c/ Google LLC*, 8 déc. 2022, n° C-460/20, §68 et 72. Dans cet arrêt, la liberté d'information est même totalement passée sous silence

l'intervention préalable d'une décision de justice – à charge pour le demandeur du déréférencement de prouver l'inexactitude manifeste.

D'autre part, la portée géographique du droit au déréférencement est circonscrite. En 2014, elle était limitée au seul pays du demandeur – Google n'était contraint de déréférencer l'adresse URL que pour le pays dans lequel réside l'utilisateur faisant jouer son droit au déréférencement. Cette portée est néanmoins redéfinie en 2019 par la CJUE pour s'étendre l'ensemble de l'UE – le déréférencement mis en œuvre à la demande d'un utilisateur européen vaut pour tout le territoire de l'UE⁶³³. Cette décision ouvre même aux États membres la possibilité d'attribuer une portée mondiale à un tel déréférencement à l'issue d'une mise en balance entre le droit au respect de la vie privée et la liberté d'information, en laissant aux États et aux autorités nationales de contrôle le pouvoir souverain de définir les conditions qui justifient un déréférencement mondial⁶³⁴.

Le droit au déréférencement est aussi plus récemment protégé par la Cour européenne des droits de l'Homme (Cour EDH), sur une ligne assez similaire à celle de la CJUE mais bien plus pusillanime à l'égard des souverainetés nationales. En juin 2021, la Cour EDH considère qu'il n'est pas nécessaire de rechercher d'équilibre entre la liberté d'information et la liberté d'expression lorsque la demande de déréférencement de données personnelles est émise par une autre personne que celle concernée par ces données⁶³⁵. Ces deux libertés n'entrent en conflit que si la personne concernée par une atteinte à sa vie privée exerce son droit au déréférencement. En novembre 2021, la Cour de Strasbourg statue pour la première fois sur une demande de déréférencement émise par des citoyens européens⁶³⁶. En l'espèce, deux participants à une bagarre dans un restaurant avaient demandé à l'éditeur en chef d'un journal de déréférencer un article édité par ce journal qui avait relaté les faits en nommant les

633CJUE, *Google LLC c/ CNIL*, 2019, §68-69 : « il résulte notamment des articles 56 et 60 du [RGPD] que, pour les traitements transfrontaliers, (...) les différentes autorités de contrôle nationales concernées doivent coopérer (...) afin de parvenir à un consensus et à une décision unique qui lie l'ensemble de ces autorités et dont le responsable du traitement doit assurer le respect en ce qui concerne les activités de traitement menées dans le cadre de tous ses établissements dans l'Union. Par ailleurs, l'article 61 (...) oblige les autorités de contrôle notamment à se communiquer les informations utiles et à se prêter mutuellement assistance en vue de mettre en œuvre et d'appliquer ce règlement de façon cohérente dans l'ensemble de l'Union (...). / Ce cadre réglementaire fournit ainsi aux autorités de contrôle nationales les instruments et les mécanismes nécessaires (...) pour pouvoir adopter, le cas échéant, une décision de déréférencement qui couvre l'ensemble des recherches effectuées sur la base du nom de cette personne à partir du territoire de l'Union ».

634Ibid., §72 : « si (...) le droit de l'Union n'impose pas (...) que le déréférencement auquel il serait fait droit porte sur l'ensemble des versions du moteur de recherche en cause, il ne l'interdit pas non plus. Partant, une autorité de contrôle ou une autorité judiciaire d'un État membre demeure compétente pour effectuer, à l'aune des standards nationaux de protection des droits fondamentaux (...), une mise en balance entre, d'une part, le droit de la personne concernée au respect de sa vie privée et à la protection des données à caractère personnel la concernant et, d'autre part, le droit à la liberté d'information, et, au terme de cette mise en balance, pour enjoindre, le cas échéant, à l'exploitant de ce moteur de recherche de procéder à un déréférencement portant sur l'ensemble des versions dudit moteur. ». En réponse, le juge administratif français considère que, le législateur français n'ayant pas conféré à la CNIL le pouvoir de faire déréférencer des résultats au-delà du champ prévu par le droit de l'UE, la CNIL ne peut pas ordonner un déréférencement qui excéderait le territoire de l'UE : Conseil d'État, *Google Inc.*, 27 mars 2020, n° 399922

635Cour EDH, *Hurbain c/ Belgique*, 22 juin 2021, n° 57292/16, §127

636Cour EDH, *Biancardi c/ Italie*, 25 nov. 2021, n° 77419/16

protagonistes. Les juridictions nationales obligent l'éditeur à déréférencer l'article litigieux et à payer à chaque protagoniste 5 000 euros en dédommagement moral du traitement de données à caractère personnel effectué par le journal. L'éditeur conteste la décision nationale devant la Cour EDH. La Cour distingue ici la suppression d'un article de son déréférencement. Par « suppression d'un article », la Cour EDH désigne la suppression de sa source de publication (blog, journal...). Au contraire, le déréférencement désigne la suppression de son chemin d'accès depuis un moteur de recherche, auquel cas l'article demeure accessible en ligne sur sa source de publication (site web sur lequel est publié l'article). En présence d'une suppression d'articles contenant des informations sur une personne identifiable, la Cour EDH applique classiquement sa jurisprudence *Axel Springer* de février 2012. Elle évalue la conciliation de la liberté d'expression (art. 10 de la Convention) et du droit à la vie privée (art. 8) selon six critères⁶³⁷. En revanche, en présence d'un déréférencement, la Cour EDH évalue la conciliation de la liberté d'expression et du droit à la vie privée selon trois critères : la durée pendant laquelle l'article était en ligne ; la sensibilité des données personnelles en cause ; et enfin la gravité de la sanction imposée au requérant⁶³⁸. La liberté d'expression, telle qu'elle doit être conciliée avec le droit à la vie privée, inclut aussi la liberté d'information⁶³⁹.

Chapitre 2. Les techniques de blocage et de filtrage de l'accès

Le blocage et le filtrage figurent parmi les techniques de restriction les plus utilisées pour contrôler l'échelle de diffusion d'une donnée en ligne, tant dans le passé qu'actuellement. Cette popularité s'explique probablement par leurs avantages, qui permettent d'imposer une restriction radicale à un grand nombre de prescripteurs numériques tout en ciblant précisément les données à restreindre, mais elle s'explique aussi par les nombreuses déclinaisons du blocage (masquage de données, désactivation d'une fonctionnalité, bannissement partiel ou total...) et par l'action préventive du filtrage.

Sur le plan juridique, le blocage et le filtrage offrent aussi aux États de restreindre, pour leur population respective, l'accès à une donnée hébergée à l'étranger sans porter atteinte aux compétences souveraines de l'État étranger dont le territoire accueille la donnée bloquée ou filtrée. Ainsi, le blocage et le filtrage évitent à la fois des conflits de compétence et diplomatiques tout en restreignant l'accès d'une donnée depuis le seul territoire de l'État qui décide le blocage ou le filtrage. On examinera d'abord le blocage (Section 1) avant de nous concentrer sur le filtrage (Section 2).

⁶³⁷Cour EDH, *Axel Springer c/ Allemagne*, 7 fév. 2012, n° 39954/08, §89-95. Les critères sont les suivants : la contribution de l'article à un débat d'intérêt public ; la notoriété de la personne visée et l'objet de l'article (par exemple une condamnation pénale) ; le comportement de la personne visée à l'égard des médias (si elle a ou non fait les démarches pour rendre elle-même publiques les informations en cause) ; le mode d'obtention des informations et leur véracité ; le contenu, la forme et les répercussions de la publication (y compris le degré de diffusion) ; et enfin la gravité de la sanction (la gravité de l'atteinte portée à la liberté d'expression du requérant).

⁶³⁸Cour EDH, *Biancardi c/ Italie*, 2021, §64-69

⁶³⁹Dans l'affaire *Hurbain c/ Belgique* précitée, la Cour rappelle ainsi que « les droits d'une personne ayant fait l'objet d'une publication disponible sur l'internet doivent (...) être mis en balance avec le droit du public à s'informer sur des événements du passé et de l'histoire contemporaine, notamment à l'aide des archives numériques de la presse » (§107), sachant que « ce sont en effet les moteurs de recherche qui mettent les archives en lumière » (§59)

Section 1. La technique du blocage

On examinera le recours au blocage, pratiqué tant au niveau de la transmission que du stockage de données (Paragraphe 1), avant de spécialiser l'étude sur le blocage des contenus et des logiciels (Paragraphe 2), et enfin sur le blocage de certaines fonctions logicielles à travers l'étude de cas de TikTok en Russie (Paragraphe 3).

Paragraphe 1 – Le blocage de la transmission et du stockage de données

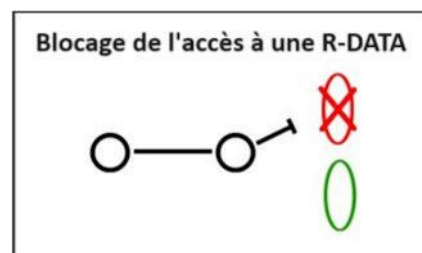
Le blocage sera examiné d'après notre grille de lecture classique, en étudiant d'abord le blocage mis en oeuvre dès la transmission (A), puis celui mis en oeuvre dès le stockage dans le cadre d'un bannissement total (B) ou partiel (C) d'un utilisateur.

A) Le blocage dès la transmission

1. Le blocage dès l'acheminement en Chine et en Russie

On a vu deux techniques de restriction spécifiques aux infrastructures de transmission de données – la coupure et le ralentissement. Le blocage de l'accès à des données est une technique praticable aussi bien auprès des infrastructures de transmission qu'auprès des supports de stockage de données (terminal, serveur et périphériques accessoires). On étudie d'abord le blocage dès la transmission.

On appelle « blocage de l'accès à une R-DATA » la technique consistant, depuis le nœud récepteur, à empêcher le nœud émetteur d'accéder à une R-DATA déjà stockée sur internet. Cette technique peut difficilement être utilisée sur les moyens de transport car elle nécessite de savoir, dès le transport, si les données peuvent être ou non transmises à la machine destinataire. Pour que des données soient bloquées dès le transport, il faudrait donc que soient analysées toutes les données transportées, puis que soit détecté et empêché le transport de celles d'entre elles qui aboutissent une R-DATA. Or, la vitesse du trafic transporté varie de 200 000km/s (vitesse du courant électrique, pour le transport par câbles terrestres électriques) à 299 000km/s (vitesse de la lumière, pour le transport par voie aérienne, satellitaire et par fibre optique terrestre et sous-marine). La vitesse du traitement de données (analyse, détection, décision de blocage) devra donc être à peu près égale à la vitesse de la lumière *pour chaque donnée* transportée, sans quoi le traitement de données ralentira gravement le trafic au point de congestionner le réseau voire de le rendre inutilisable. Cette prouesse n'est pas possible techniquement à ce jour, de façon que le blocage ne peut intervenir sur les moyens de transport.



Il en va différemment des moyens d'acheminement. Par sa fonction même, le moyen d'acheminement doit de toute façon traiter les requêtes d'accès qui lui parviennent pour les diriger vers la route pertinente. En cas de blocage, les requêtes d'accès sont, à l'occasion de leur traitement, empêchées d'être dirigées vers des routes qui mènent au destinataire bloqué. Le blocage peut survenir sous plusieurs modalités : en bloquant l'adresse IP destinataire mentionnée dans le datagramme IP de la requête d'accès (blocage par adresse IP) ; en bloquant le nom du réseau local du destinataire (blocage par noms d'hôtes) ; en bloquant le nom de domaine du destinataire (blocage par DNS) ; en bloquant l'adresse URL destinataire (blocage par URL) ... Lorsque le blocage est effectué dès l'acheminement, le routeur occupe la position du nœud émetteur par rapport au nœud destinataire dont il bloque l'accès. Afin de mener des blocages,

les opérateurs s'équipent d'une ou plusieurs bases de données dites « listes noires » qui répertorient les nœuds destinataires bloqués⁶⁴⁰. En pratique, lorsqu'il mentionne un destinataire (adresse IP, URL, nom de domaine...) figurant dans la liste noire stockée par le routeur, tout paquet IP qui emprunte ce routeur est empêché de poursuivre sa route.

Le blocage dès l'acheminement est par exemple très recouru par l'État en Chine. On a vu que, à travers son article 5, un règlement de 1997 définit pour la première fois les neuf catégories de contenus interdits de diffusion par les utilisateurs sur le sol chinois⁶⁴¹. L'article 10 de ce règlement rend les FAI responsables « *d'établir un réseau entièrement sécurisé, protégé et bien géré* » et de « *retirer du réseau l'adresse du répertoire ou du serveur dont le contenu viole l'art. 5* », L'article 20 sanctionne d'une amende de 15 000 yuans l'opérateur qui viole ces dispositions et, en cas d' « *infraction grave* », menace d'une fermeture pendant six mois du réseau du particulier ou de l'opérateur défaillant, d'un retrait de la licence d'exploitation qui permet à l'opérateur de fournir ses services sur le territoire, ou de l'annulation de l'inscription de l'opérateur sur le réseau sur décision de la Sécurité Publique – soit des menaces de coupure dans toutes ces hypothèses. « *Par peur d'être sanctionnés* » face à la largesse de ces dispositions (« responsabilité d'établir un réseau entièrement bien géré », « infraction grave »...) et à la gravité de la sanction (perte de la licence d'exploitation et bannissement du marché de la fourniture d'accès), les opérateurs « *ajoutent un deuxième niveau de censure, en créant généralement à leur tour leur propre liste noire* »⁶⁴².

Ce régime juridique conduit à un système d'autocensure par lequel les opérateurs initient eux-mêmes une intense régulation paraétatique et renforcent le blocage. En 2002, une étude de l'Université de droit de Harvard dénombre 18 000 sites web bloqués en Chine⁶⁴³. En 2020, une équipe de chercheurs issue de quatre universités américaines et canadienne rapporte 311 000 noms de domaine bloqués par les opérateurs sur le sol chinois⁶⁴⁴. Sont notamment bloqués des

640V. par ex., en France, REES Marc, « Sites miroirs et listes noires, derniers préparatifs avant l'An 1 de l'ARCOM », *NextInPact*, 29 déc. 2021

641Conseil des affaires de l'État, Règlement sur la sécurité, la protection et la gestion des réseaux d'information et d'Internet (计算机信息网络国际联网安全保护管理办法) du 30 déc. 1997. Les contenus d'information interdits par l'art. 5 sont ceux qui : « (i) sont contraires aux principes fondamentaux énoncés dans la Constitution ; (ii) portent atteinte à la sécurité nationale, divulguent les secrets d'État, constituent une menace pour le gouvernement ou pour l'unité de la nation ; (iii) nuisent l'honneur et aux intérêts de l'État ; (iv) incitent à la haine ou à la discrimination ethniques ou nuisent à l'unité nationale ; (v) vont à l'encontre des politiques de l'État en matière de religion, ou qui contribuent à la promotion d'organisations hérétiques, de croyances féodales et de superstitions ; (vi) répandent des rumeurs qui perturbent l'ordre social ou menacent la stabilité sociale ; (vii) diffusent des informations à caractère pornographique ou licencieux, encouragent le jeu, la violence, l'homicide et la terreur, ou incitent à commettre des crimes ; (viii) propagent des informations insultantes ou diffamatoires, ou qui portent atteinte aux droits et intérêts légitimes d'autrui ; (iv) sont contraires à la loi ou aux règlements administratifs » (liste actuelle, telle que révisée par l'ordonnance n° 292 du Conseil des affaires de l'État de septembre 2000 pour y insérer la référence aux secrets d'État)

642BAYEN-POISSON Aurélie « Cybercontrôle en Chine : l'omni-surveillance à l'ère du numérique » [en ligne], *La Revue des Médias*, 21 déc. 2018

643ZITTRAIN Jonathan et EDELMAN Benjamin, « Empirical Analysis of Internet Filtering in China » [en ligne], *Berkman Center for Internet & Society*, Harvard Law School, 2003

644HOANG Nguyen Phong, NIAKI Arian Akhavan, DALEK Jakub, KNOCKEL Jeffrey, LIN Pellaeon, MARCZAK Bill, CRETE-NISHIHATA Masahi, GILL Phillipa et POLYCHRONAKIS

réseaux sociaux (Twitter, Facebook, Reddit, Quora, Snapchat, Instagram, Tumblr, Pinterest, Tinder...), des services de streaming (Netflix, YouTube, Dailymotion, Twitch, Spotify, Soundcloud, Pornhub et services pornographiques en général...), des services de messagerie (Gmail, WhatsApp, Facebook Messenger, Telegram, Signal, Viber, Zoom, parfois Skype...), des services de presse (New York Time, Wall Street Journal, Financial Times, Le Monde...), des moteurs de recherche (Google, Alexa, DuckDuckGo...), des services de blogging (Blogspot, WordPress, Medium, Tumblr...) etc.

En Russie, c'est en 2012 que l'État attribue à une administration – le Roskomnadzor⁶⁴⁵ – le pouvoir d'obliger les opérateurs à pratiquer des blocages. Jusqu'à cette date, la décision de blocage pouvait seulement provenir de l'autorité judiciaire contre les services ou contenus illicites énumérés par l'art. 4 de la loi de 1991 sur les médias⁶⁴⁶. Le Roskomnadzor ne pouvait pas lui-même ordonner le blocage de sites, mais adresser des avertissements écrits aux fondateurs de médias de masse privés⁶⁴⁷ qui permettent la diffusion de contenus interdits par l'art. 4⁶⁴⁸. Après avoir adressé deux avertissements à un même fondateur au cours de la même année, le Roskomnadzor peut saisir le juge judiciaire, lequel statue sur la cessation ou non de

Michalis, « How Great is the Great Firewall? » [en ligne sur arXiv], *30th USENIX Security Symposium*, 2021, p. 3381-3398

645 Les compétences du Roskomnadzor (Service fédéral de supervision des communications, des technologies de l'information et des médias de masse) s'appliquent à tous les médias de masse, en ligne ou non, et recouvrent celles de l'Arcep (gestion des fréquences hertziennes), de la Cnil (protection des données personnelles), de l'Arcom (régulation du secteur audiovisuel et des communications au public en ligne), de l'OCLCTIC (pédopornographie et terrorisme en ligne) et de l'Arjel (Autorité de régulation des jeux en ligne) françaises.

646 Loi fédérale n° 2124-I relative aux médias de masse (Закон о средствах массовой информации) du 27 décembre 1991. Initialement, l'art. 4 de la loi de 1991 condamnait seulement trois catégories de contenus : la commission d'actes criminels en ligne, la divulgation de secrets d'État, et la diffusion, l'incitation ou la promotion en ligne d'activités terroristes. S'y sont progressivement ajoutées neuf autres catégories de contenus interdits : la promotion de la pornographie, du culte de la violence, de la cruauté et de l'obscénité (ajouté par la loi fédérale n° 114-FZ du 19 juil. 1995) ; la diffusion par la vidéo ou la radio d'informations affectant le subconscient des personnes et/ou ayant un effet néfaste sur leur santé (même loi) ; les méthodes de développement, de fabrication et d'utilisation de produits stupéfiants ainsi que des lieux de leur acquisition (loi fédérale n° 90-FZ du 20 juin 2000) ; les contenus extrémistes autres que terroristes (loi fédérale n° 112-FZ du 25 juil. 2002) ; la diffusion par les médias de techniques et de tactiques susceptibles d'entraver la conduite d'une opération terroriste ou de mettre en danger la vie et la santé des personnes (la loi fédérale n° 153-FZ du 27 juillet 2006) ; les informations identifiantes sur un mineur victime d'actes illicites (loi fédérale n° 50-FZ du 5 avril 2013) ; la proposition de vente d'alcool ou de produits alimentaires alcoolisés (loi fédérale n° 278-FZ du 29 juil. 2017) ; les reportages et documents portant sur les ONG étrangères enregistrées ou non-enregistrées, ou sur un individu enregistré en qualité d'agent étranger, ainsi que les documents créés par ces ONG ou individus lorsqu'ils n'indiquent pas exercer en qualité d'agents étrangers (loi fédérale n° 481-FZ du 30 décembre 2020) ; les instructions sur la fabrication et la modification improvisée d'explosifs et d'armes, y compris d'armes à feu (loi fédérale n° 370-FZ du 28 juin 2021).

647 L'art. 2 de la loi relative aux médias de masse définit les médias de masse comme « toute forme de distribution périodique d'informations de masse », et définit l'information de masse comme « les messages et matériels (...) destinés à un nombre illimité de personnes ». Les opérateurs et services internet intègrent cette définition, mais les services internet font l'objet d'une catégorie spécifique – la « publication en ligne » définie comme « tout site de réseaux d'informations et de télécommunications sur internet inscrit en qualité de société de médias de masse » – depuis la loi n° 170-FZ modifiant certains actes législatifs de la Fédération de Russie en vue d'améliorer la législation applicable au secteur de l'information de masse du 11 juin 2011.

648 Loi relative aux médias de masse, art. 16

l'activité du fondateur sur le territoire russe, par retrait de son certificat d'enregistrement de média de masse⁶⁴⁹.

En 2012, une loi fédérale modifie la loi sur l'information de 2006 pour y introduire un nouvel art. 15.1⁶⁵⁰. Cet article charge le Roskomnadzor de tenir un registre qui répertorie tous les noms de domaines, adresses URL et noms d'hôtes de sites internet hébergeant des contenus illicites. Les contenus répertoriés peuvent être illicites en vertu : de décisions de justice ayant ordonné la restriction de contenus particuliers (sur le fondement de l'art. 4 de la loi sur les médias) ; d'ordonnances par un huissier de restreindre l'accès à des informations diffamatoires ; de décisions du pouvoir exécutif⁶⁵¹. Cette dernière possibilité a permis le développement d'une liste administrative de contenus illicites pour le Roskomnadzor (art. 15.1 de la loi sur l'information), parallèle à la liste des contenus illicites valant pour un litige devant le juge non initié par le Roskomnadzor (art. 4 de la loi sur les médias). Ainsi, l'art. 15.1§5 définit cette liste administrative en énonçant un ensemble de contenus à restreindre devant figurer dans le registre du Roskomnadzor, ensemble qui n'a cessé de s'enrichir avec le temps⁶⁵². Si l'hébergeur d'un service ne restreint pas l'accès d'un contenu illicite dans un délai de 24h après que le Roskomnadzor ait notifié l'illicéité de ce contenu à cet hébergeur, tous les opérateurs sur le territoire russe sont obligés de bloquer l'accès aux adresses indexées dans le registre de

649RICHTER Andrei et RICHTER Anya, *Réglementation des contenus en ligne en Fédération de Russie?*, Observatoire européen de l'audiovisuel, 2015 : « *Le principal instrument [du Roskomnadzor pour contrôler les violations de l'art. 4] est l'avertissement (...). En 2013, le Roskomnadzor a adressé 21 avertissements "anti-extrémistes" aux services de rédaction de diverses publications. SOVA Center, l'une des principes ONG russes qui traite des questions relatives au discours de haine, (...) mentionne 8 avertissements relatifs à la publication de la vidéo interdite des Pussy Riot [lors] de leur prestation à la cathédrale du Christ St-Sauveur de Moscou* »

650Loi fédérale n° 139-FZ modifiant la loi fédérale sur la protection des mineurs contre les l'informations nuisibles à leur santé et à leur développement et certains actes législatifs de la Fédération de Russie ("О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации) du 28 juillet 2012. L'amendement de la loi relative à l'information de 2006 intervient dans le cadre d'une loi essentiellement destinée à modifier la loi n° 436-FZ sur la protection des mineurs du 29 déc. 2010 (laquelle prévoyait initialement une classification des tranches d'âge pour l'accès à l'information, de type 9+, 12+, 14+, 18+...). Les pouvoirs de blocage ont donc été attribués au Roskomnadzor dans un contexte législatif ayant pour principal objet la protection en ligne des mineurs.

651Loi fédérale n° 149-FZ relative à l'information, aux technologies de l'information et à la protection de l'information ("Об информации, информационных технологиях и о защите информации") du 27 juil. 2006, art. 15.1§5

652En 2012, les adresses à bloquer figurant sur le registre pouvaient restreindre l'accès à trois types de contenus : la pédopornographie ; les méthodes et appels au suicide ; et la promotion de stupéfiants et substances psychotropes. La liste s'est étendue à six autres catégories : aux informations identifiantes sur un mineur victime d'actes illicites (loi fédérale N° 50-FZ du 5 avril 2013) ; aux informations qui enfreignent la législation russe sur les jeux de hasard et les loteries (loi fédérale n° 222-FZ du 21 juil. 2014) ; à la proposition de vente d'alcool ou de produits alimentaires alcoolisés (loi fédérale n° 278-FZ du 29 juil. 2017) ; aux informations visant à inciter ou à impliquer de quelque manière des mineurs dans la commission d'actes illégaux qui constituent une menace pour leur vie et/ou leur santé et/ou la santé d'autrui (loi n° 472-FZ du 18 décembre 2018) ; les offres de commerce de détail de médicaments par des personnes qui n'ont pas de licence et d'autorisation, ou dont la vente au détail est restreinte ou interdite (loi n° 105-FZ du 3 avril 2020) ; aux méthodes pour la fabrication et la modification improvisée d'explosifs et d'armes, y compris d'armes à feu (loi n° 288-FZ du 1^{er} juillet 2021)

l'autorité administrative⁶⁵³. Cette modification de 2012 est un tournant pour l'internet russe, car les compétences du Roskomnadzor s'étendent quasiment à toutes les communications illicites en ligne et à tous les opérateurs sur le territoire russe. Par conséquent, l'obligation de blocage par les opérateurs se généralise à tous les contenus illicites indexés par le Roskomnadzor dans son registre qui n'ont pas été restreints par les hébergeurs dans un délai de 24h après leur notification par le Roskomnadzor. En 2016, le Roskomnadzor avait inscrit 88 500 sites et pages web d'après son rapport annuel d'activité de 2017⁶⁵⁴. Ce chiffre est toutefois très irrégulier : le 17 juin 2020, le doctorant à l'université d'Oxford Lincoln Pigman recense 650 000 adresses IP inscrites dans le registre du Roskomnadzor alors que le réseau social de messagerie Telegram était bloqué depuis 2018 ; après le Roskomnadzor ait ordonné le déblocage de Telegram le 18 juin 2020, le nombre d'adresses IP inscrites dans le registre chute à un peu plus de 30 000⁶⁵⁵.

1. Le blocage dès l'acheminement en France, au Royaume-Uni et aux États-Unis

En France, jusqu'en 2015, seule une décision judiciaire pouvait obliger l'opérateur à bloquer l'accès à un service ou à un contenu sur le fondement de l'art. 6, I, 8 LCEN (contre tout contenu occasionnant ou susceptible d'occasionner un dommage) ou de l'art. L336-2 du Code de la propriété intellectuelle (contre toute atteinte à un droit d'auteur). Depuis 2015, le législateur a confié le pouvoir d'ordonner le blocage à deux autorités administratives, estimant la procédure judiciaire trop lente pour lutter efficacement contre la diffusion de certaines infractions en ligne⁶⁵⁶. La première, l'OCLCTIC, est dépendante du pouvoir exécutif et précisément du ministère de l'Intérieur puisque rattachée à la sous-direction de la lutte contre la cybercriminalité, un organisme de la police créé en août 2014⁶⁵⁷. En novembre 2014, le législateur accorde à l'OCLCTIC le pouvoir d'obliger les opérateurs à bloquer l'accès aux hébergeurs qui n'ont pas supprimé de leurs services, dans un délai de 24h, les contenus pédopornographiques et à caractère terroriste ou en faisant l'apologie leur ayant été notifiés par

653Loi fédérale relative à l'information, aux technologies de l'information et à la protection de l'information de 2006, art. 15.1§10

654WIJERMARS Mariëlle et LEHTISAARI Katja, *Freedom of Expression in Russia's New Mediasphere*, Paragraphe « Managing the Blacklist » du chapitre 2 « The blacklisting mechanism », Routledge, 2019

655PIGMAN Lincoln, « In memoriam: Russia's ban on Telegram, 2018-2020 », *Riddle Russia*, 22 juin 2020

656Assemblée nationale, Rapport n° 2173 sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, 22 juil. 2014, p. 27 : le rapporteur de la loi justifie les pouvoirs de blocage confiés à la première administration (OCLCTIC) par le but de « *donner davantage d'efficacité à la lutte des pouvoirs publics contre la propagande terroriste sur Internet* » ; Sénat, Rapport n° 557 sur le projet de loi relatif à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique et sur le projet de loi organique modifiant la loi organique n° 2010 relative à l'application du cinquième alinéa de l'article 13 de la Constitution, 5 mai 2021, p. 29 : le rapporteur justifie les pouvoirs de blocage confiés à la deuxième administration (Arcom) par le fait que « *les titulaires des droits se retrouvent démunis et découragés quand, au terme d'une action judiciaire qui a pu s'étaler sur plusieurs mois, le site fermé réapparaît quelques jours plus tard*. Or, la protection de la liberté d'expression contraint fortement l'autorité administrative pour ordonner des mesures de blocage, et l'autorité judiciaire ne peut par nature procéder systématiquement dans l'urgence nécessaire » (souligné par le rapport).

657Loi n° 1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, art. 12

l'OCLCTIC. La deuxième administration dotée d'une prérogative de blocage est une autorité administrative indépendante : l'Arcom (Autorité de régulation des communications audiovisuelles et numériques). Issue de la fusion du CSA et de la Hadopi, elle naît en janvier 2022 avec le pouvoir d'établir une liste noire des « *services portant atteinte, de manière grave et répétée, aux droits d'auteur ou aux droits voisins* », et d'obliger les opérateurs à bloquer l'accès aux services figurant sur la liste noire en-dehors de toute procédure judiciaire⁶⁵⁸. L'Arcom a ordonné le blocage de l'accès à plus de 400 services de streaming illicites entre janvier et avril 2022, principalement des services diffusant illégalement des compétitions sportives. Quant à l'OCLCTIC, elle avait adressé 439 demandes de blocages de services hébergeant des contenus pédopornographiques et à caractère terroriste sur l'année 2021⁶⁵⁹. Contrairement à la Chine, les opérateurs français ne peuvent pas être tenus pour responsables de leur trafic à moins de l'avoir volontairement manipulé⁶⁶⁰. Par ailleurs soumis au principe de neutralité d'internet, les opérateurs ont peu de champ pour pouvoir pratiquer des blocages parallèlement à ceux requis par les autorités judiciaires et administratives, et risquent d'engager leur responsabilité en prenant eux-mêmes la décision de modifier le trafic.

Au Royaume-Uni, jusqu'en 2011, seule une décision judiciaire pouvait obliger l'opérateur à bloquer l'accès à un service ou à un contenu⁶⁶¹. En octobre 2011, le gouvernement britannique admet le blocage par les opérateurs sans passer par la voie judiciaire à travers à code pratique d'adhésion volontaire qu'il supervise, signé par les quatre principaux opérateurs (BT, TalkTalk, Virgin Media et Sky), et destiné à « *bloquer les contenus dommageables* » (tels que ceux « *promouvant le suicide, l'anorexie, le jeu, l'automutilation et la violence, la séduction sexuelle en ligne ou la cyberintimidation* »)⁶⁶². Les opérateurs qui y adhèrent s'engagent « *donner à tous les nouveaux abonnés un choix actif d'appliquer ou non des contrôles (...) pour bloquer les contenus dommageables* ». Après un discours du 22 juillet 2013 du Premier ministre David Cameron exigeant un blocage « *par défaut (...) des contenus pour adulte (...) seulement pour les*

658Code de la propriété intellectuelle, article L331-25 issu de la loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique. Le blocage d'un service ne peut être décidé qu'après comparution en séance publique du service concerné, dans le cadre d'une procédure accusatoire où le représentant légal du service est entendu, et après délibération de l'Arcom sur le blocage ou non de ce service.

659Pour l'Arcom, v. Arcom, « Intervention de Denis Rapone à la table ronde de l'Arcom et du Centre national du cinéma : Protection de la création » et le document joint « En chiffres. Le partage de contenus sportifs et culturels » [en ligne sur le site de l'Arcom], *Festival de Cannes 2022*, 23 mai 2022. Pour l'OCLCTIC, v. CNIL, « Rapport d'activité 2021 de la personnalité qualifiée », mai 2022, p. 11

660L'irresponsabilité des opérateurs posée par l'art. 12 de la directive « commerce électronique » est conditionnée par la neutralité de leur rôle de transport et d'acheminement en qualité d'« *intermédiaires techniques* »

661Généralement sur le fondement de l'art. 97A du *Copyright, Designs and Patents Act* du 15 novembre 1988, qui reconnaît à la Haute Cour le pouvoir d'adresser une injonction à l'encontre d'un fournisseur de services ayant effectivement connaissance de ce qu'autrui utilise son service pour enfreindre le droit d'auteur

662Département britannique de l'Éducation, « Parents asked if adult websites should be blocked », sur *Gov.uk*, 28 juin 2012. Depuis les années 1990, le Royaume-Uni régule le réseau internet à l'aide de codes pratiques d'adhésion volontaires (généralement émis par l'Office of Communications (Ofcom), équivalant à une fusion de l'Arcep et de l'Arcom françaises) : v. AKDENIZ Yaman, « The Regulation Of Pornography And Child Pornography On The Internet. », *Journal of Information, Law and Technology*, 1997.

nouveaux abonnés », le message est compris à la lettre par les opérateurs signataires du code de conduite de 2011. Ils interprètent le « choix actif d'appliquer ou non des contrôles » comme un système de blocage et de filtrage par défaut, que les abonnés majeurs peuvent lever en procédant à des démarches identifiantes auprès de l'opérateur ⁶⁶³. Ainsi, fin 2013, cette procédure de blocage et de filtrage par défaut est appliquée pour tous les nouveaux abonnés des quatre opérateurs signataires⁶⁶⁴, qu'ils ont progressivement étendue aux anciens abonnés⁶⁶⁵. Le blocage de l'acheminement de contenus dommageables est généralisé.

Enfin, aux États-Unis, le Premier Amendement limite doublement la possibilité pour la Fédération et les États fédérés d'obliger les entreprises privées à employer des techniques de restriction : il ne protège largement la liberté d'expression que contre des ingérences gouvernementales, ce qui prive les États du pouvoir d'intervenir dans l'expression de chacun sur le réseau⁶⁶⁶ ; et il protège moindrement la liberté d'expression contre les ingérences privées, ce qui confère aux entreprises privées la liberté de choisir la régulation des contenus applicable sur leurs services sans que ces choix portent atteinte à la liberté d'expression de chacun⁶⁶⁷. Aussi, la conciliation de la section 230 avec une responsabilisation des plateformes en qualité de régulateurs est un casse-tête aux États-Unis depuis la promulgation de ce texte en 1996⁶⁶⁸. Le cumul du Premier Amendement et de la section 230 rend très difficile de tenir les acteurs privés responsables par principe d'obligations de blocage, de filtrage, de ralentissement ou de toute autre restriction. Pour cette raison, nous n'avons trouvé aucune trace d'obligation de

⁶⁶³Par exemple, l'opérateur TalkTalk fournit à ses abonnés l'outil de protection par défaut HomeSafe, qui comporte lui-même l'outil KidSafe. KidSafe propose à ses abonnés de restreindre 9 catégories de contenus : « drogues et techniques criminelles », « partage de fichiers et hacking », « jeux d'argent », « contenus inappropriés », « jeux en ligne », « vie privée et vol d'identité », « réseaux sociaux », « suicide et automutilation », « armes et violence, gore et haine ». Les abonnés indiquent les restrictions qui valent pour l'ensemble des machines connectées au réseau du foyer familial (v. la rubrique « How tu use Homesafe » sur le site de TalkTalk). L'opérateur Sky propose à l'abonné de paramétrer le Sky Broadband Shield selon l'un des trois niveaux d'âge suivants : les enfants de moins de 13 ans (niveau « PG », qui bloque dix catégories de contenus – hameçonnage et logiciels malveillants ; rencontres en ligne ; logiciels anonymisant ; partage de fichier et hacking ; drogues et techniques criminelles ; armes, violence, gore et haine ; adulte ; suicide et automutilation ; réseaux sociaux ; jeux en ligne) ; les adolescents (niveau 13, qui bloque les mêmes catégories de contenus à l'exception des réseaux sociaux et des jeux en ligne) ; les adultes de 18 ans (niveau 18, qui bloque seulement la catégorie hameçonnage et logiciels malveillants). V. les rubriques « How tu use Homesafe » sur le site de TalkTalk et « Using Sky Broadband Shield » sur le site de Sky.

⁶⁶⁴IGLEZAKIS Ioannis, *The Legal Regulation of Cyber Attacks*, Kluwer Law International B.V., 2020

⁶⁶⁵VINCENT James, « BT to introduce default "porn filtering" » [en ligne], *The Independent*, 16 déc. 2013 ; WESTAWAY Luke, « Sky Broadband to start filtering adult content by default » [en ligne], sur *CNET*, 20 janv. 2015

⁶⁶⁶Cour Suprême des États-Unis, *Reno v. ACLU*, 521 U.S. 844 (1997)

⁶⁶⁷Par ex., *Nyabwa v. Facebook*, CIVIL ACTION NO. 2:17-CV-24 (S.D. Tex. Jan. 26, 2018)

⁶⁶⁸Le Président des États-Unis Donald Trump avait promis d'abroger avant la fin de son mandat la section 230 qu'il jugeait incompatible avec une responsabilisation des plateformes, telle qu'une obligation de neutralité politique vis-à-vis des contenus publiés (« Responsabilités des réseaux sociaux : les États-Unis renoncent à la réforme de la "section 230" », *Le Monde*, 2021, en ligne). Durant ses promesses de campagnes, le Président Joe Biden s'est engagé à réviser la section 230 que lui aussi juge incompatible avec la responsabilisation des plateformes, telle l'obligation d'agir contre la désinformation notamment dans le contexte de la pandémie de Covid19 (« Social media liability law is likely to be reviewed under Biden », *The Washington Post*, 2021).

blocage dès l'acheminement dans la législation fédérale des États-Unis. Les juges états-uniens ont certes le pouvoir de bloquer des services ou des contenus dans le cadre de litiges par des ordonnances de blocage valant *inter-partes*⁶⁶⁹. Même sur décisions de justice ou dans le cadre d'enquêtes, les blocages étatiques dès l'acheminement sont très rares.

Par rapport à la coupure, le blocage offre comme le ralentissement l'avantage de pouvoir cibler une catégorie de services, de programmes ou de contenus. Cette technique est donc très adaptée aux R-DATA qui couvrent de tels objets. Par ailleurs, contrairement au ralentissement, elle ne se limite pas à décourager l'accès à une R-DATA mais empêche cet accès, ce qui provoque une réduction immédiate de l'échelle de diffusion d'une R-DATA. Ainsi, après avoir bloqué 400 services de streaming illicite, l'Arcom constate une diminution immédiate de 37% de l'audience sportive illicite globale en France sur internet⁶⁷⁰. On a vu néanmoins que le blocage peut être associé au ralentissement si le routeur bloqueur ralentit la requête au point d'en faire expirer la validité. L'association des deux présente le double intérêt d'épuiser la patience du prescripteur souhaitant accéder à la R-DATA bloquée par ralentissement, et d'empêcher *in fine* cet accès. Cependant, cette association des techniques ne comble pas la principale faiblesse commune au ralentissement et au blocage, à savoir la facilité de leur contournement à moyen et long terme voire à court terme, contrairement à la coupure. En effet, toutes les informations bloquées (adresse IP, URL, nom de domaine, nom d'hôte...) peuvent être modifiées par le prescripteur qui fait stocker des R-DATA au moyen de logiciels masquant l'adresse IP, de services intermédiaires modifiant les informations bloquées (réseaux privés virtuels (VPN), darknets⁶⁷¹...), ou encore de changement par les services de leur nom de domaine et/ou de leur serveur d'hébergement.

De plus, comme la coupure et le ralentissement, le blocage peut engendrer un fort risque de sur-blocage (situation de blocage de A-DATA par ricochet au blocage de R-DATA). Le blocage de l'adresse IP du serveur sur lequel est hébergé un service illégal engendre le blocage de tous les services hébergés sur ce même serveur⁶⁷² ; le blocage d'un nom de domaine illégal engendre le blocage de tous les sous-domaines qui en découlent⁶⁷³ ; le blocage d'une adresse URL peut

⁶⁶⁹ Par ex., Cour fédéral du District Sud de New-York, *United King Distributors et al. v. Israeli-tv.com et v. Israel.tv*, No 1:2021cv11025, 26 avr. 2022 (blocage de plateformes de streaming illicite d'œuvres protégées)

⁶⁷⁰ Arcom, « Intervention de Denis Rapone à la table ronde de l'Arcom et du CNC », 2022, préc.

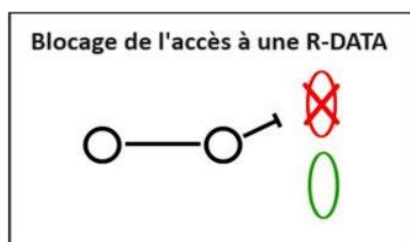
⁶⁷¹ Un darknet est un réseau qui superpose ses propres protocoles réseau, anonymisants, par-dessus les protocoles du réseau internet. Par exemple, le darknet TOR utilise le protocole IP pour la communication, mais y superpose des protocoles de nœuds bénévoles : les utilisateurs de TOR peuvent bénévolement prêter l'adresse IP de leur machine ; l'utilisateur de TOR emprunte les nœuds bénévoles pour accéder au serveur ou au terminal destinataire, et se connecte à celui-ci au moyen de l'adresse IP du dernier nœud bénévole emprunté.

⁶⁷² Par exemple, le blocage par l'Argentine d'un blog divulguant des secrets d'État (leakymails.blogspot.com) a provoqué le blocage de la totalité du service « Blogger » qui l'hébergeait et du million de blogs hébergés par ce service, partageant la même adresse IP : YORK Jillian C., « Argentine ISPs Use Bazoooka to Kill Fly » [en ligne], sur *Electronic Frontier Foundation*, 19 août 2011

⁶⁷³ Ainsi, le blocage par les États-Unis d'un service pédopornographique ayant pour sous-domaine ***.mo00.com a provoqué le blocage des 84 000 autres services en ligne partageant le sous-domaine mo00.com : REES Marc, « Pédopornographie : 84 000 sites bloqués et accusés par erreur » [en ligne], *NextInPact*, 17 févr. 2011

engendrer le blocage de tout le service qui redirige vers cette adresse URL⁶⁷⁴... Sur un plan juridique, dans le Conseil de l'Europe, le sur-blocage peut entraîner des violations de la liberté d'expression et des droits des propriétaires des services collatéralement victimes du blocage de services tiers⁶⁷⁵. L'obstacle posé au sur-blocage par le respect des droits individuels n'existe pas en Chine, où l'interprétation constitutionnelle priorise classiquement les droits de l'État lorsqu'ils contredisent ceux de l'individu⁶⁷⁶. Ainsi, l'étude inter-universitaire précitée a évalué que 13% des services bloqués en Chine l'étaient accidentellement⁶⁷⁷. Sur un plan économique, nous n'avons pas trouvé d'études scientifiques évaluant l'impact du sur-blocage auprès d'un marché, d'autant que cet impact varie sans doute selon les parts de ce marché que détenaient les services avant leur sur-blocage. En revanche, un sur-blocage prive un marché de l'apport économique potentiel ou actuel de services licites voire intégrés dans ce marché. Par exemple, l'association britannique spécialisée dans les droits en ligne Open Rights Group conclut en 2014 que le blocage par défaut au Royaume-Uni provoque un sur-blocage de 20% des sites les plus populaires et que 96% des sites bloqués ne sont pas à caractère pornographique (tandis que D. Cameron promettait un blocage par défaut des seuls « *contenus pour adultes* »)⁶⁷⁸. En 2019, l'Open Rights Group compte plus de 8 000 domaines bloqués par ce dispositif, dont plus de 1 300 ont été débloqués, « *suggérant que de nombreux sites web ont été et restent censurés à tort* »⁶⁷⁹.

B) Le blocage du stockage de données : l'exemple du bannissement total par blocage



La technique de blocage n'est pas seulement praticable au stade de la transmission de données, mais aussi au stade du stockage de données par les serveurs et les terminaux. La configuration est la même que pour le blocage de l'acheminement : le nœud récepteur empêche le nœud émetteur d'accéder à une R-DATA déjà hébergée sur internet. Toutefois le nœud récepteur qui bloque l'accès est incarné cette fois non plus par un routeur, mais par un serveur.

⁶⁷⁴ Ainsi, le blocage par le Royaume-Uni d'une URL de Wikipédia qui renvoyait à l'image de couverture de l'album *Virgin Killer* de Scorpions (1976) a provoqué le blocage de la page entière sur Wikipédia et l'impossibilité technique pour les utilisateurs d'éditer un article sur wikipedia.en : REES Marc, « UK : Wikipédia piquée par l'un des scorpions du filtrage », *NextInPact*, 8 déc. 2008

⁶⁷⁵ Cour EDH, *Ahmet Yildirim c. Turquie*, 18 déc. 2012, n° 3111/10 (viole l'art. 10 de la Convention le blocage d'un blog hébergé par Google qui entraîner le blocage du service Google, lequel n'était pas visé par la mesure) ; Cour EDH, *Cengiz e. a. c. Turquie*, 1^{er} déc. 2015, n° 18226/10 et 14027/11 (le blocage sans base légale viole l'art. 10) ; Cour EDH, *OOO Flavus and others versus Russia*, n° 12468/15, 23 juin 2020, 23489/15 et 19074/16 (viole l'art. 10 et les « *droits des propriétaires de sites internet* » le blocage qui affecte « *collatéralement* » un site internet non visé par la mesure de blocage)

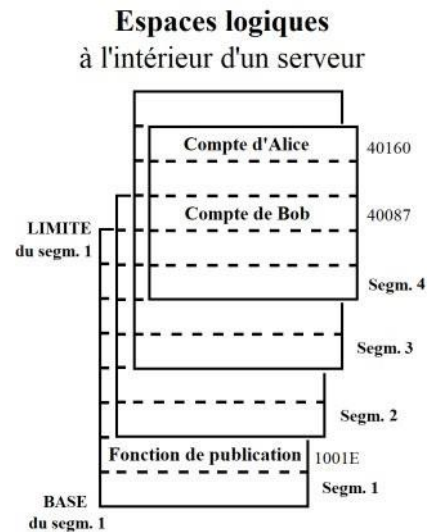
⁶⁷⁶ WANG Hao, « The conceptual basis of privacy standards in China and its implications for China's privacy law », *Frontiers of Law in China*, vol. 7, 2012, p. 147

⁶⁷⁷ HOANG Nguyen Phong, NIAKI Arian Akhavan, DALEK Jakub, KNOCKEL Jeffrey, LIN Pellaeon, MARCZAK Bill, CRETE-NISHIHATA Masahi, GILL Phillipa et POLYCHRONAKIS Michalis, « How Great is the Great Firewall? » [en ligne sur arXiv], *30th USENIX Security Symposium*, 2021, p. 3381-3398

⁶⁷⁸ CHAMPEAU Guillaume, « Près de 20 % des sites les plus populaires sont bloqués en GB », *Numerama*, 4 juil. 2014

⁶⁷⁹ MIGLIANO Simon, « ISP Website Blocks: How Bad are the UK's Web Filters?" Blocking in the UK », *Open Rights Group* et *TOP10VPN*, avr. 2019

Lorsqu'il est pratiqué par un serveur, le blocage consiste à empêcher l'accès d'un nœud émetteur à un ou plusieurs espaces logiques. On appelle « espace logique » un espace mémoire qui accueille des données numériques. On a vu que, dans les ordinateurs contemporains, toutes les données sont stockées dans des « segments mémoire virtuels ». Prenons l'exemple d'une application qui propose à ses utilisateurs une fonction de publication de leurs contenus. On entre dans la mémoire du serveur qui héberge la base de données de ladite application : imaginons que le 1^{er} segment mémoire de ce serveur contienne la référence à la fonction de publication des contenus, que la référence au compte utilisateur d'Alice soit présente dans les 3^e et 4^e segments, et que la référence au compte utilisateur de Bob soit présente dans les 2^e, 3^e et 4^e segments (ci-contre).



Chaque octet présent dans un segment possède une adresse dite « logique », qui permet d'appeler l'exécution de cet octet. Pour simplifier le lecture du schéma, on a rapporté l'ensemble des octets constitués par la fonction de publication à une même adresse logique (1001E) ; on a fait de même pour les comptes d'Alice et Bob (adresses logiques 40087 et 40160 sur le segment 4). En empêchant un utilisateur d'accéder à l'adresse logique 1001E, on l'empêche alors de pouvoir utiliser la fonction de publication sur l'application concernée. De même, en empêchant l'adresse 40087 du segment 4 (et les adresses logiques correspondantes sur les segment 2 et 3) de communiquer avec l'adresse 40160 (et l'adresse logique correspondante sur le segment 3), on empêche au compte de Bob d'accéder au compte d'Alice. Chacune de ces données est autorisée à être hébergée, et l'est effectivement, mais est inaccessible à l'utilisateur bloqué.

Bloquer l'accès à des données depuis le serveur qui les héberge permet ainsi de cloisonner les différents espaces logiques qui constituent une application : empêcher Bob de contacter Alice sur la même application, empêcher Alice d'utiliser la fonction de publication, empêcher Bob d'accéder à une discussion de groupe, empêcher un utilisateur non-inscrit d'accéder aux fonctionnalités de messagerie de l'application, l'empêcher d'accéder à certaines pages web de l'application... Dès lors, **le blocage de l'accès à des données depuis le serveur qui les héberge offre l'avantage de pouvoir contrôler le type de données accessibles à un ou plusieurs utilisateurs**, tandis que **le blocage dès l'acheminement permet de contrôler la destination accessible à un ou plusieurs utilisateurs**.

Le blocage peut aussi être effectué par un autre serveur que le serveur hébergeant les données bloquées. Dans ce cas, ce serveur tiers n'a pas de contrôle sur l'espace mémoire occupé par les données problématiques, et ne peut donc pas choisir précisément les espaces logiques à bloquer. Il ne peut bloquer que la destination (URL, nom de domaine, nom d'hôte du serveur, nom d'hôte du terminal...), *i.e.* l'accès à la machine qui héberge les données problématiques. **Le blocage de l'accès à des données depuis un serveur tiers partage donc le même inconvénient que le blocage dès l'acheminement : il se limite à bloquer une destination.** Cela se traduit par une **aggravation du risque de sur-blocage**. En effet, faute de pouvoir cibler précisément les espaces logiques contenant les données problématiques, le blocage depuis un serveur tiers ne peut cibler qu'un vaste espace logique, à savoir la totalité de l'espace mémoire occupé par le

destinataire. Si le destinataire bloqué est une URL, sera bloqué l'accès à la page web correspondante ; si le destinataire bloqué est un nom de domaine, sera bloqué l'accès à l'application qui porte ce nom ; si le destinataire bloqué est le nom d'hôte d'un serveur, sera bloqué l'accès à toutes les applications hébergées par ce serveur etc.

Cependant, le blocage depuis un serveur tiers possède un avantage important vis-à-vis du blocage dès l'acheminement : contrairement au routeur, le serveur tiers peut être entièrement consacré à héberger un service de blocage, qui détaille les modalités du système de blocage. Autrement dit, **par rapport au blocage dès l'acheminement, le blocage depuis un serveur tiers a pour avantage de sophistiquer le système de blocage.** Par ailleurs, contrairement au blocage depuis le serveur hébergeant les données problématiques, le blocage depuis un serveur tiers a certes pour inconvénient de ne pas offrir un contrôle précis des espaces logiques qui contiennent ces données, donc de ne pas offrir un contrôle des types de données accessibles. Néanmoins, **par rapport au blocage de l'accès à des données depuis le serveur qui les héberge, le blocage depuis un serveur tiers a aussi son avantage : il permet de bloquer l'accès à des données sans le consentement de l'exploitant du serveur qui héberge ces données.** Il est alors possible pour le régulateur de déployer tout un réseau de serveurs tiers dédié à un système de blocage, pour empêcher l'accès à telle ou telle application en ligne, telle ou telle page web, tel ou tel terminal, sans nécessiter la coopération de qui que ce soit d'autre que le régulateur. On verra que cette option a d'ailleurs été activée en Russie, à travers son réseau national de noms de domaines, et qu'elle est en cours d'activation en France et au Royaume-Uni dans une moindre mesure, à travers une plateforme dédiée au blocage de l'accès des mineurs aux applications pornographiques.

Dans le cadre de cette sous-partie, on examine spécifiquement un type de blocage : celui dirigé contre un ou plusieurs utilisateurs pour les empêcher d'accéder aux données bloquées. Dans ce cas, le blocage a pour effet de bannir l'utilisateur d'un espace logique, ce qui rentre dans le champ de la technique de « bannissement » qu'on a déjà croisée.

On a vu qu'un utilisateur peut être banni *par suppression de données*, auquel cas les données associées à cet utilisateur sont éliminées de l'espace mémoire des serveurs hébergeant lesdites données. Un utilisateur peut aussi être banni *par blocage de données*, auquel cas cet utilisateur est empêché depuis un serveur d'accéder à un espace logique hébergé par le serveur destinataire. On étudie ici le cas dans lequel un utilisateur est empêché d'accéder à la totalité de l'espace logique occupé par l'application.

Il en va ainsi des serveurs qui bannissent les enfants des applications pornographiques. C'est la voie dans laquelle s'engage le droit britannique depuis plusieurs années pour lutter contre l'accès des mineurs à la pornographie en ligne. En 2017, dans le cadre d'un projet de loi sur l'économie numérique, le Parlement britannique envisage d'obliger les fournisseurs de services pornographiques en ligne à vérifier efficacement l'âge de leurs utilisateurs au risque d'être bloqués⁶⁸⁰. Le mécanisme privilégié proposait qu'une plateforme tierce, s'intercalant entre l'utilisateur et le service pornographique, vérifie la condition de l'âge à l'aide d'une carte bancaire ou d'identité de façon à ne pas laisser ces informations entre les mains des services pornographiques ; ceux de ces services qui auraient refusé de passer par cette plateforme encourraient le blocage dès l'acheminement sur le territoire britannique. Le dispositif consiste

680BROWN Thomas, « Digital Economy Act 2017 (Commencement of Part 3) Bill [HL] », sur *Lordslibrary.parliament.uk* (site web de la Bibliothèque de la chambre des Lords), 19 janv. 2022

donc à bloquer, dès les serveurs hébergeant la plateforme intermédiaire, l'accès des jeunes utilisateurs à une R-DATA (« contenus pornographiques ») hébergée sur les serveurs des applications pornographiques. En 2019, le projet est reporté *sine die*, puis reprend en février 2022 dans le cadre d'un projet de loi sur la sécurité en ligne. Afin de limiter le risque de sur- blocage (blocage de services sans rapport avec le service litigieux mais hébergés sur le même serveur bloqué), le gouvernement conditionne désormais le blocage d'un service récalcitrant par le refus persistant de ce service *après* qu'il ait été condamné à une amende pouvant s'élever à 10% de son chiffre d'affaires mondial⁶⁸¹. N'est toutefois pas résolu le problème de protection des données personnelles : quelle entreprise ou administration (gestionnaire de la plateforme intermédiaire) peut être autorisée à connaître l'identité civile et les heures de connexion de tous les consommateurs britanniques de pornographie en ligne ? Le projet est suspendu en juillet 2022 après la démission du Premier Ministre Boris Johnson.

Les ambitions britanniques inspirent un député français qui, lors d'une séance de questions au gouvernement en mai 2019, demande à ce dernier s'il a « *l'intention de mettre en place rapidement un système similaire [à celui du Royaume Uni] afin de protéger les enfants de ces contenus inappropriés* »⁶⁸². En novembre 2019, le président de la République Emmanuel Macron annonce son exigence que les services pornographiques en ligne adoptent des techniques de filtrage « *efficaces et réelles* » pour empêcher leur utilisation par des mineurs, sans indiquer les techniques en question⁶⁸³. En février 2023, le ministre français délégué chargé de la Transition Numérique annonce qu'un dispositif de blocage sera instauré d'ici la fin de l'année 2023 : les internautes français devront préalablement, sur une plateforme tierce, remplir un certificat anonyme attestant de leur majorité, et ne pourront accéder aux applications pornographiques qu'au moyen de ce certificat de majorité numérique⁶⁸⁴. Dans le cas britannique comme français, le bannissement consiste à bloquer, depuis un serveur tiers, l'accès des jeunes internautes à l'espace des applications pornographiques.

Outre le cas des enfants et des sites pornographiques, de nombreuses applications (jeux vidéo, places de marché, plateformes de diffusion ou de partage de vidéos, messageries instantanées, sites de rencontres, forums, wikis et autres réseaux sociaux) ont développé des mécanismes de « suspension de comptes » contre leurs utilisateurs violant les règles légales ou la politique de l'application. Les données du compte suspendu sont alors toujours hébergées par le serveur, mais les informations d'authentification du compte de cet utilisateur (nom d'utilisateur, mot de passe, voire adresse mail, numéro de téléphone...) sont blacklistées, indexées dans une base de données en qualité de

681LAUSSON Julien, « Le Royaume-Uni essaie une nouvelle fois de forcer les sites pornos à vérifier l'âge des internautes », *Numerama*, 8 fév. 2022

682Assemblée Nationale française, Séance de questions au gouvernement du 21 mai 2019, sur [Questions.assemblee-nationale.fr](https://questions.assemblee-nationale.fr)

683REES Marc, « Protection des mineurs : le plan de bataille de Macron contre le porno en ligne », *NextInPact*, 20 nov. 2019 ; « Pornographie en ligne : trois questions sur les mesures souhaitées par Macron pour protéger les jeunes », *France Info*, 22 nov. 2019

684« Sites pornographiques : cinq questions sur "l'attestation numérique" que le gouvernement envisage d'instaurer pour bloquer l'accès aux mineurs », *France Info*, 6 fév. 2023 ; CORDIER Solène, « Le gouvernement étudie les pistes pour restreindre l'accès des mineurs aux sites pornographiques », *Le Monde*, 7 fév. 2023 ; LEBELLE Aurélie, POUPEAU Thomas et LOMBART Gaël, « Sites pornos : un dispositif pour vraiment bloquer l'accès aux mineurs », *Le Parisien*, 6 fév. 2023

« compte suspendu » ⁶⁸⁵ . Chaque fois que l'utilisateur insérera ses identifiants, le serveur hébergeant la base de données bloquera ainsi l'accès de cet utilisateur aux autres informations de la base de données – donc lui bloquera l'accès à l'ensemble de l'application. Une suspension de compte a donc pour effet de bannir le compte de cet utilisateur, provisoirement ou définitivement, de la totalité de l'espace logique occupé par l'application qui le suspend.

Le bannissement ne repose pas nécessairement sur des informations qui authentifient l'identité civile d'un utilisateur (dans les cas britannique et français) ou son identité sur un service en ligne (dans le cas d'une suspension de compte). Il peut aussi reposer sur des informations qui authentifient la géolocalisation d'un utilisateur. Par exemple, depuis sa création en 2007, l'application de vidéos à la demande Hulu (concurrent direct de Netflix, entre 40 et 50 millions d'utilisateurs actifs/mois) bloque l'utilisation de sa plateforme depuis d'autres emplacements géographiques que les États-Unis et le Japon.

C) *Le blocage du stockage de données : l'exemple du bannissement partiel par blocage*

Le bannissement par blocage peut aussi viser à bannir l'utilisateur d'une ou plusieurs parties de l'espace logique total occupé par l'application – on parlera de « bannissement partiel ». Le bannissement partiel peut d'abord mis en œuvre à l'initiative du propriétaire de l'application (donc de l'exploitant des serveurs hébergeant son application).

Outre le cas d'Hulu, le blocage par géolocalisation est aussi pratiqué depuis mars 2022 par le réseau social TikTok, par crainte de participer à la diffusion de « fausses informations » au sens de la loi russe, donc par crainte de se voir bloqué ou filtré dès l'acheminement sur décision du Roskomnadzor. Le blocage par géolocalisation est aussi pratiqué depuis mars 2022 par le réseau social TikTok, par crainte de participer à la diffusion de « fausses informations » au sens de la loi russe, donc par crainte de se voir bloqué ou filtré dès l'acheminement sur décision du Roskomnadzor. En Russie, tout fournisseur de publication en ligne risque déjà, depuis 2019, d'être bloqué ou filtré dès l'acheminement sur ordre du Roskomnadzor s'il participe à la diffusion d' « *informations non fiables ayant un impact significatif sur la société et mettant en danger la vie et/ou la santé des citoyens, menaçant de perturber massivement l'ordre public et/ou la sécurité intérieure, ou menaçant d'interférer ou de perturber des infrastructures vitales* » ⁶⁸⁶ . Ces dispositions sont néanmoins complétées le 4 mars 2022, moins de dix jours après l'invasion de l'Ukraine par l'armée russe le 24 février, pour inclure parmi les fausses informations celles « *délibérément fausses sur les forces armées russes* » ⁶⁸⁷ . Or, l'administration russe qualifie son intervention en Ukraine d' « *opération militaire* » et juge comme étant une fausse information la qualification d' « *invasion* » relayée par de nombreux médias étrangers. Dans ces conditions, empêcher la diffusion de fausses informations

685V. par ex. « Locking and Unlocking User Accounts », sur *docs.oracle.com*. Oracle est un fournisseur d'hébergement, principalement connu pour ses serveurs d'hébergement de bases de données

686Loi fédérale n° 31-FZ modifiant l'article 15.3 de la loi fédérale « sur l'information, les technologies de l'information et la protection de l'information » (Федеральный закон "О внесении изменений в статью 15.3 Федерального закона "Об информации, информационных технологиях и о защите информации") du 18 mars 2019, 1) et 2)

687Loi fédérale n° 32-FZ sur les amendements au Code pénal de la Fédération de Russie et aux articles 31 et 151 du Code de procédure pénale de la Fédération de Russie (Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации") du 4 mars 2022, art. 1^{er}

conformément à la loi russe nécessite d'empêcher l'accès à tous les médias qui relaient ladite qualification d'invasion, ou n'importe quel message dénigrant l'armée ou les stratégies militaires russes.

Pour s'adapter à cette loi, TikTok annonce à ses utilisateurs le 6 mars 2022 qu'il suspend la publication de toute nouvelle vidéo par des utilisateurs russes. Le 8 mars, sans en informer le public, le réseau social de courtes vidéos bloque l'accès des internautes russes à toute vidéo et à tout compte TikTok étranger (y compris au compte TikTok de l'ONU ⁶⁸⁸). Ce blocage par géolocalisation a été révélé par l'équipe de chercheurs Tracking Exposed⁶⁸⁹. Le recours à cette technique assure à TikTok de se conformer à la loi russe, offrant ainsi au réseau social l'opportunité de rester légalement présent sur le marché russe et d'y conserver sa base d'utilisateurs et ses revenus (notamment publicitaires)⁶⁹⁰. Les mesures prises par TikTok se sont traduites par une légère diminution de sa base d'utilisateurs, mais surtout par une brusque interruption de sa croissance : de 29 millions début 2021, le nombre d'utilisateurs actifs mensuels de TikTok atteint 57-60 millions en février 2022, la veille de l'intervention russe, puis décroît à 50-55 millions en septembre 2022⁶⁹¹. La croissance de TikTok semble toutefois reprendre progressivement en Russie depuis octobre-novembre 2022 (55-65 millions d'utilisateurs actifs/mois)⁶⁹². Cela illustre à la fois : la difficulté du nouveau « TikTok russe », instrument de propagande, à convaincre davantage d'utilisateurs dans les mois qui ont suivi la transformation du réseau social ; et la conservation par TikTok de sa base d'utilisateurs russes.

Inversement, les applications qui n'ont pas bloqué l'accès de leurs utilisateurs aux informations des médias étrangers (BBC, Deutsche Welle, Facebook, Instagram, Twitter, Google News, Meduza...) se sont vues elles-mêmes bloquées dès l'acheminement sur décision du Roskomnadzor. Ainsi, le nombre d'utilisateurs actifs mensuels d'Instagram, qui s'élevait à 65 millions en janvier 2022 (avant le blocage subi par Instagram en mars 2022), a chuté à 26 millions en septembre 2022 – ce qui signifie que 26 millions d'utilisateurs russes ont contourné cemois-ci le blocage par les routeurs russes. Plus impressionnant, le nombre d'utilisateurs actifs mensuels de Facebook, qui s'élevait à 73 millions en janvier 2022 (avant le blocage subi par Facebook en mars

⁶⁸⁸ BATEMAN Tom, « TikTok's ban on foreign content in Russia 'risks turning it into a propaganda platform' », sur *Euronews.com*, 17 mars 2022

⁶⁸⁹ LELOUP Damien, « TikTok accusé d'offrir un "passe-droit" aux propagandistes du Kremlin », *Le Monde*, 15 mars 2022

⁶⁹⁰ Outre la conservation de ses revenus, la régulation menée par TikTok s'explique peut-être aussi par la pression de l'État chinois. En effet, sur le territoire chinois, l'État a ordonné aux principaux réseaux sociaux de bloquer eux aussi l'accès à des informations qui dénigreraient l'armée russe : CHANG Gordon G., « China's TikTok Is Russia's New Disinformation Machine », *Newsweek*, 25 mars 2022

⁶⁹¹ « Share of TikTok monthly user reach in Russia in August 2021, by age group and gender », sur *Statista.com*, sept. 2022 (v. le texte en légende) ; KEMP Simon, « Digital 2022: The Russian Federation », sur *Datareportal.com*, 15 fév. 2022 ; et v. sur les bases de données de Semrush l'évolution du nombre de visiteurs uniques de TikTok entre janv. et sept. 2022 sur le territoire russe (*Semrush.com*), croisée avec la base de données de SimilarWeb retraçant l'évolution du nombre de visites uniques de TikTok durant la même période (*Similarweb.com*)

⁶⁹² V. sur la base de données de Semrush l'évolution du nombre de visiteurs uniques de TikTok sur le territoire russe ; et « Monthly number of users of social networks in Russia in November 2022, by platform », sur *Statista.com*, mars 2023

2022), a dégringolé à 8 millions en septembre 2022⁶⁹³. Quant aux médias d'information BBC et Meduza (journal russe indépendant), on estime que le nombre de leurs utilisateurs actifs mensuels a respectivement chuté de 12-15 millions (février 2022) à 4,5-6 millions (mars 2023) et de 6-7 millions (février 2022) à 4-5 millions (en mars 2023)⁶⁹⁴.

Le bannissement partiel peut ensuite être mis en œuvre à l'initiative, non du propriétaire de l'application ou d'un État, mais des utilisateurs. Dans ce cas, le propriétaire de l'application met à disposition des utilisateurs des outils de bannissement partiel. Par exemple, sur Twitch, TikTok, YouTube, Twitter, Instagram ou encore Snapchat, l'utilisateur qui administre un espace de discussion de type chat (espace de messagerie instantanée, *i.e.* en temps réel, ouvert à plusieurs participants) peut bannir de cet espace tout utilisateur tiers dont il ne souhaite pas voir les messages⁶⁹⁵. Sur les mêmes réseaux sociaux, tout utilisateur peut aussi bloquer l'accès, aux utilisateurs indésirables, de son espace personnel de messagerie (les empêchant d'envoyer des messages à l'utilisateur bloqueur), de son espace personnel d'expérience (empêchant les contenus produits ou relayés par l'utilisateur bloqué de figurer parmi les contenus proposés à l'utilisateur bloqueur) et/ou de son profil (empêchant l'utilisateur bloqué de consulter les contenus affichés sur le profil de l'utilisateur bloqueur, de s'abonner au compte de l'utilisateur bloqueur pour recevoir ses actualités, ou encore de mentionner l'utilisateur bloqueur sur Instagram).

Le type de bannissement approprié – partiel ou total – dépend de la source de provenance de la R-DATA. **Si la R-DATA** (cyberharcèlement, commentaires haineux, informations étrangères...) **provient d'une ou plusieurs parties de l'application** (groupe de discussion, espace de commentaires, comptes et contenus étrangers...), **le bannissement partiel sera le plus approprié**. En revanche, **si la R-DATA est indissociable de l'usage généralement fait d'une application par un utilisateur ou une catégorie d'utilisateurs** (la R-DATA « accès des mineurs à la pornographie » est indissociable des utilisateurs mineurs, la R-DATA « harcèlement » est indissociable de l'utilisateur qui se sert de l'application pour harceler autrui quelle que soit la partie de l'application concernée...), **le bannissement total sera le plus approprié**.

Que le bannissement soit partiel ou total, on a vu qu'il peut être initié par l'application elle-même ou encore par un utilisateur qui possède des outils de blocage (par ex. en bloquant un autre utilisateur). Lorsque le bannissement est initié par un utilisateur, on lui voit deux principaux avantages. D'une part, l'utilisateur est le mieux positionné pour évaluer le respect de sa volonté par les autres utilisateurs (donc pour identifier les internautes indésirables), et les utilisateurs sont la catégorie d'acteurs qui contribue le plus directement à la diffusion d'une donnée. Par conséquent, **le bannissement initié par des utilisateurs permet** à ces derniers de maîtriser davantage leurs contacts avec les autres utilisateurs, donc de choisir plus intentionnellement leurs expériences en ligne, donc **de réduire l'échelle de diffusion des actions des utilisateurs non désirés**. D'autre part, le bannissement initié par l'utilisateur permet d'individualiser la mise

693 Sur ces chiffres, v. « Leading social media platforms in Russia in 3rd quarter 2022, by monthly penetration rate », sur *Statista.com*, 20 mars 2023 ; MELKADZE A, « Number of Facebook users in Russia monthly 2020-2022 », sur *Statista.com*, 21 sept. 2022 ; et KEMP Simon, « Digital 2022: The Russian Federation », sur *Datareportal.com*, 15 fév. 2022

694 V. sur la base de données de Semrush l'évolution du nombre de visiteurs uniques de BBC.com et Meduza.io sur le territoire russe entre février 2022 et mars 2023

695 Pour Twitch, v. « À propos des sanctions de compte et des bannissements du chat », sur *help.twitch.tv* [consulté le 13 mars 2023] ; pour Google, v. « Bloquer des spectateurs sur le chat en direct YouTube », sur *support.google.com* [consulté le 13 mars 2023] ; pour TikTok, v. « Violations du contenu et bannissements », sur *support.tiktok.com* [consulté le 13 mars 2023]

en œuvre du blocage : chaque utilisateur détenant un pouvoir de blocage, il existe autant de sources de blocage que d'utilisateurs recourant au blocage, et la réactivité du blocage dépend de l'évaluation de l'utilisateur bloqueur. L'utilisateur bloqué qui souhaite contourner le blocage se heurte donc à une multitude de sources de blocage et/ou à une réactivité immédiate lorsqu'il diffuse une R-DATA. Par conséquent, **le blocage initié par l'utilisateur rend plus difficile le contournement du blocage.**

Cette technique porte néanmoins deux inconvénients. D'une part, l'outil de bannissement ne sera mobilisé par l'utilisateur que contre des utilisateurs indésirables, ce qui en fait une technique inadaptée lorsque l'utilisateur accède volontairement à des internautes qui produisent des R-DATA (utilisateur qui visualise intentionnellement les contenus d'un internaute exposant des violations de droits d'auteur, des méthodes de suicide ou des conseils de consommation de drogues, utilisateur qui accède à un groupe de discussion à caractère terroriste...). **Le bannissement initié par l'utilisateur n'est donc pas adapté pour bannir tout internaute créateur de R-DATA, mais seulement pour bannir les internautes qui stockent des indésirables** (internautes harceleurs, créateurs de spams, de contenus haineux ou violents...). D'autre part, on pense inopportun de mettre à la disposition des utilisateurs des outils de bannissement total : cette solution confierait à un utilisateur non modérateur le pouvoir d'empêcher tout accès à une application par n'importe quel autre utilisateur. Cela créerait l'opportunité pour une communauté organisée d'utilisateurs de prendre le contrôle d'une voire plusieurs applications, en en bannissant tout utilisateur non-membre de ladite communauté. Même si les outils de bannissement total étaient réservés à une personne reconnue comme victime par la justice, et à l'encontre de la seule personne reconnue responsable du préjudice de la victime, un tel pouvoir de bannissement total ferait de la victime un organe d'application de la décision de justice qui la concerne. Dès lors, **le bannissement initié par l'utilisateur peut difficilement s'étendre au-delà du bannissement partiel.**

Le bannissement initié par l'application porte les avantages et inconvénients inverses à ceux du bannissement initié par l'utilisateur. **Le bannissement initié par l'application a pour premier avantage** de ne pas dépendre de la volonté individuelle des utilisateurs, donc **d'être adapté pour bannir tout internaute quel que soit la R-DATA concernée** (indésirable ou non). **Il a pour second avantage de pouvoir procéder aussi bien par bannissement partiel que par bannissement total** en évitant à l'application d'être l'objet de stratégies d'exclusion et de contrôle déployées par des utilisateurs. Concrètement, cela signifie que l'application est la mieux positionnée pour bannir totalement un utilisateur (suspendre son compte, lui bloquer l'accès à l'application par géolocalisation...), tandis que l'utilisateur est le mieux positionné pour bannir partiellement un autre utilisateur (l'empêcher d'accéder au compte, à la messagerie et/ou aux contenus de l'utilisateur bloqueur, d'accéder à un espace de discussion administré par l'utilisateur bloqueur...).

Outre ses avantages, le bannissement initié par l'application a toutefois pour premier inconvénient d'instaurer une source unique de blocage – la décision de l'application de bannir un ou plusieurs utilisateurs. L'utilisateur bloqué qui souhaite contourner le blocage n'a qu'une seule source de blocage à contourner et, du fait de son unicité, les failles de cette source sont exploitables par tous les utilisateurs. Dès lors, par rapport au bannissement initié par l'utilisateur, **le bannissement initié par l'application facilite le risque de contournement.** Le second inconvénient du bannissement initié par l'application découle du fait que le blocage est dans ce cas nécessairement automatisé. Cela signifie que *tous* les principes, exceptions et circonstances pertinentes d'application de la règle de blocage sont fixés *avant* la survenance d'un cas concret de blocage, sans qu'un interprète évalue la pertinence de l'application de la

règle dans ce cas concret une fois survenu. Or, dans la mesure où il est impossible de prédire toutes les circonstances dans lesquelles une R-DATA peut survenir, **le bannissement initié par l'application aggrave le risque de sur-blocage et de sous-blocage.**

Paragraphe 2 – Le blocage du stockage de contenus et de logiciels tiers

Outre le bannissement de l'utilisateur, on étudiera deux autres techniques de blocage dès le stockage de données : le blocage de contenus (A) ; et le blocage de logiciels (B).

A) Le masquage de contenus

On a vu que, s'agissant du bannissement, l'objet du blocage est l'utilisateur. Dans ce cas, un espace logique est interdit d'accès à l'internaute. Le blocage dès les serveurs peut avoir d'autres objets, notamment : les contenus (un espace logique est interdit d'accès à des contenus) ; et les logiciels (un espace logique est interdit d'accès à un logiciel). On examine d'abord le cas des contenus.

Le masquage de contenus consiste à empêcher des contenus d'apparaître auprès d'un utilisateur. Contrairement au filtrage qu'on étudiera après, le masquage de contenus n'empêche pas la production même d'un contenu, mais son accès par d'autres utilisateurs que son auteur, *i.e.* sa diffusion. Le contenu filtré n'est pas autorisé à être hébergé sur les serveurs ; le contenu masqué, effectivement hébergé par les serveurs, est autorisé à exister en ligne mais il est invisible pour le(s) seul(s) utilisateur(s) qui masque(nt) le contenu (ou qui se voi(en)t imposer un masquage de contenus).

Par rapport au bannissement, le masquage a pour avantage de pouvoir cibler les contenus. Il a en revanche pour inconvénient de ne pas pouvoir cibler des utilisateurs, contrairement au bannissement. Autrement dit, tandis que **bannissement est adapté lorsque la R-DATA provient d'un ou plusieurs internautes** identifiés, le **masquage de contenus est adapté lorsque la R-DATA provient d'un ou plusieurs contenus** identifiés. À la différence du bannissement, le masquage ne repose alors pas sur des données identifiant les utilisateurs (compte utilisateur, documents d'identité civile...), mais sur des données identifiant les contenus (texte, image, son ou vidéo porté par le contenu).

Le masquage de contenus peut procéder de deux façons : il peut invisibiliser le contenu après la visualisation de ce dernier par l'utilisateur (masquage *ex post*) ; et il peut l'invisibiliser avant sa visualisation par l'utilisateur (masquage *ex ante*). À titre d'exemples de masquage *ex post*, Twitter, LinkedIn ou encore Pinterest confèrent à leurs utilisateurs le pouvoir de masquer les contenus de façon à ne plus les afficher sur la page d'accueil ou le fil d'actualités de l'utilisateur⁶⁹⁶. Le masquage *ex post* hérite de l'avantage général du masquage, *i.e.* d'offrir la possibilité de cibler des contenus (et non des utilisateurs) pour les empêcher d'accéder à certains espaces logiques (page d'accueil, fil d'actualités...). Il a cependant pour défaut de n'agir qu'après la visualisation du contenu. N'intervenant qu'après une telle visualisation, le masquage *ex post* ne peut pas empêcher qu'un type de contenus (par ex. haineux) envahisse des fils d'actualité ou espaces commentaires, se renouvelant constamment par de nouveaux contenus et obligeant perpétuellement les utilisateurs à les masquer, assurant ainsi à ce type de contenus une échelle

⁶⁹⁶« Comment utiliser les options de masquage avancées » sur [Help.twitter.com](https://help.twitter.com/fr/masquer), « Masquer du contenu dans votre fil d'actualité » sur [Linkedin.com](https://help.linkedin.com/fr/masquer) et « Masquer ou réafficher des Épingles sur votre page d'accueil » sur [Help.pinterest.com](https://help.pinterest.com/fr/masquer)

de diffusion durablement ample. Le **principal inconvénient du masquage *ex post* réside donc dans le travail de Sisyphe auquel il donne naissance sans garantir une réduction de l'échelle de diffusion**⁶⁹⁷.

Le masquage *ex ante* corrige ce défaut de taille, en apportant l'avantage de bloquer le contenu avant sa visualisation. Ce faisant, **le masquage *ex ante* permet de bloquer un contenu avant toute amplification de son échelle de diffusion**. Cet avantage sur le masquage *ex post* s'accompagne néanmoins d'un inconvénient : par rapport au masquage *ex post* initié par l'utilisateur, **le masquage *ex ante* aggrave le risque de sur-filtrage**. En effet, le masquage *ex ante* est nécessairement automatisé, *i.e.* qu'il ne fait pas intervenir d'interprète pour évaluer l'application à l'espèce de la règle du masquage. Cela signifie que le système de masquage *ex ante* doit prévoir tous les principes, exceptions et circonstances pertinentes d'application de la règle de masquage. Or, on a vu qu'il est impossible pour un programme de prévoir et donc de couvrir exactement les circonstances dans lesquelles peut survenir une R-DATA. Cette impossibilité augmente alors le risque que des contenus licites soient accidentellement couverts par les critères de masquage, donc censurés auprès des utilisateurs masqueurs.

À titre d'exemple du masquage *ex ante*, la plupart des fils d'actualité trient aujourd'hui les contenus communiqués à l'utilisateur, donc masquent un grand nombre de contenus aux utilisateurs. Dans ce cas, le masquage est initié par l'application et empêche des contenus de parvenir aux utilisateurs. Le masquage *ex ante* peut aussi être initié par l'utilisateur. Par exemple, les internautes peuvent télécharger des logiciels appelés « adblockers » (bloqueurs de publicités) qui permettent d'invisibiliser les contenus publicitaires sur la page web visitée par l'internaute. Un bloqueur de publicités enregistre, dans sa base de données, les scripts (bouts de code) les plus couramment utilisés pour la diffusion de publicités, puis en empêche l'accès depuis sa base de données. De cette façon, les contenus publicitaires sont masqués avant même leur visualisation par l'internaute. Le bloqueur de publicités peut prendre la formes de « plugins » pour navigateur (*i.e.* des extensions logicielles d'un navigateur, comme Adblock Plus, uBlockOrigin, AdBlock...), d'applications dédiées au blocage de publicités (AdGuard, Wipr, AdLock...), d'applications plus généralistes de sécurité et de préservation de la vie privée (NextDNS, Aura...), de VPN (Surfshark, NordVPN, CyberGhost, Windscribe...) ou de navigateurs qui masquent par eux-mêmes les contenus publicitaires sans recourir à une extension logicielle (Brave Browser, Kiwi Browser, Lunascape, Polarity, Vivaldi...).

Lorsqu'il est initié par l'application, le masquage (*ex post* comme *ex ante*) hérite des avantages et inconvénients de tout blocage initié par l'application, à savoir : la possibilité de couvrir toutes les R-DATA, indésirables ou intentionnelles (1^{er} avantage) ; le risque de contournement facilité

⁶⁹⁷Les avantages et inconvénients qu'on propose sur les différentes techniques de régulation sont évalués dans l'absolu, hors de toute circonstance concrète. On verra que ces avantages et inconvénients sont très relatifs dans les faits, et que la pertinence d'une technique de régulation dépend des circonstances d'espèce. Par exemple, le filtrage de caractères permet théoriquement de prévenir l'échelle de diffusion du contenu, mais cette technique est souvent mobilisée pour censurer des données auxquelles sont attachés les utilisateurs, ce qui suscite un puissant mouvement de contournement, et relativise donc largement la réduction espérée de l'échelle de diffusion. Inversement, le masquage *ex post* est plus difficile à contourner par les personnes dont les contenus sont masqués, de sorte que le recours au masquage *ex post* pourrait réduire l'échelle de diffusion d'un contenu plus efficacement que le filtrage de caractères.

de contournement par l'établissement d'une source unique de masquage (1^{er} inconvénient) ; le risque aggravé de sur-blocage ou de sous-blocage (2^e inconvénient).

De même, lorsqu'il est initié par l'utilisateur, le masquage hérite des avantages et inconvénients de tout blocage initié par l'utilisateur. Côté inconvénients, le masquage initié par l'utilisateur n'est adapté que contre les contenus indésirables, donc inadapté contre les contenus illicites volontairement consultés par les utilisateurs. Côté avantages, il complique la possibilité de contournement par rapport au masquage initié par l'application. En effet, lorsque les internautes initient le masquage d'un contenu, le contenu masqué peut l'être par une multitude de sources de blocage, ce qui rend les sources de blocage plus éparpillées et imprévisibles. On verra un peu plus loin que l'imprévisibilité des sources de masquage peut d'ailleurs être encore renforcée en limitant au maximum la connaissance, par l'utilisateur masqué, du fait que ses contenus sont masqués⁶⁹⁸.

Malgré ces avantages et inconvénients qu'on retrouve aussi dans le bannissement, on note une forte différence entre le masquage *ex ante* et le bannissement : alors que le bannissement rend possible le blocage total de l'accès d'un utilisateur à une application pour l'empêcher d'y produire ou d'y diffuser des contenus, le masquage *ex ante* ne peut pas empêcher l'utilisateur de produire des contenus mais peut seulement l'empêcher de les diffuser (en les invisibilisant *ex ante* auprès des autres utilisateurs). Cette différence ne se répercute pas profondément sur les avantages et inconvénients du masquage *ex ante* initié par l'application. En effet, lorsque le masquage *ex ante* est initié par l'application, l'application peut décider de masquer les contenus d'un utilisateur auprès de plusieurs voire de tous les utilisateurs, ce qui certes laisse à l'utilisateur le pouvoir de produire des contenus, mais l'empêche de les diffuser sur l'application. Que l'on soit en présence d'un masquage initié par l'application ou d'un bannissement total, l'utilisateur est dans les deux cas privé de sa liberté d'utiliser l'application pour y produire ou y diffuser des contenus. Masquage *ex ante* initié par l'application et bannissement total partagent donc l'avantage d'empêcher un utilisateur d'utiliser librement une application mais, toutes deux automatisées, et partagent aussi l'inconvénient d'aggraver le risque de sur-blocage.

La différence étudiée entre le bannissement total (empêcher la production et la diffusion) et le masquage *ex ante* (empêcher la diffusion) se répercute toutefois plus profondément sur les avantages et inconvénients du masquage initié par l'utilisateur. Un **double avantage** se dégage spécifiquement **du masquage *ex ante* initié par l'utilisateur** : cette technique **permet à la fois d'intervenir avant l'échelle de diffusion tout en ne menaçant pas la liberté d'autrui d'utiliser internet**. En effet, lorsque le masquage *ex ante* est initié par l'utilisateur contre les contenus créés ou relayés par un autre utilisateur, il ne prive pas ce dernier du pouvoir de produire ou de diffuser des contenus. Il se contente d'invisibiliser, pour lui et lui seul, les contenus masqués avant toute visualisation de sa part. Contrairement au bannissement initié par l'utilisateur dont on a vu qu'il peut devenir dangereux s'il s'étend à un pouvoir de bannissement total, le masquage initié par l'utilisateur peut librement et pleinement s'exercer contre les contenus sans empêcher les autres internautes d'utiliser eux-mêmes librement l'application. De cette façon, contrairement au bannissement total, le masquage *ex ante* initié par l'utilisateur ne

⁶⁹⁸Cette méthode est aussi valable pour le bannissement initié par les utilisateurs pour renforcer l'imprévisibilité des sources de blocage, mais il est généralement plus difficile de dissimuler à l'utilisateur un bannissement de son compte (même partiel) plutôt qu'un masquage de ses contenus

peut pas être instrumentalisé pour restreindre la liberté des autres utilisateurs. Le **double inconvénient du masquage *ex ante*** initié par l'utilisateur réside toutefois qu'il **ne peut pas couvrir tous les contenus mais seulement ceux indésirables**, et qu'il **aggrave le risque de sur-blocage ou de sous-blocage** en raison de la nature automatisée de tout masquage *ex ante*.

On applique notre analyse à deux cas de masquage : le blocage de commentaires par Instagram, et le *Kids Only Safety Act* (KOSA) en préparation aux États-Unis. Depuis 2016, Instagram donne la possibilité à ses utilisateurs d'établir leur propre liste de caractères censurés (mots, émojis...) de façon à masquer tout commentaire sous leurs publications qui comporte au moins un des caractères censurés⁶⁹⁹. Le masquage développé par Instagram a ceci d'original qu'il impose le masquage du commentaire à tous les utilisateurs, sauf à l'auteur du commentaire. Ce masquage *ex ante* a donc pour avantage de maximiser la réduction de l'échelle de diffusion en censurant préventivement auprès de tous les utilisateurs les commentaires comportant des caractères censurés préétablis.

Néanmoins, le masquage *ex ante* mis en œuvre par Instagram peut être aisément contourné : il suffit à l'utilisateur masqué de créer un deuxième compte, de vérifier à l'aide de ce deuxième compte si ont été masqués les commentaires de son premier compte, d'en déduire les caractères et suites de caractères censurés, et enfin de publier des commentaires indésirables ne contenant pas ces caractères. Inversement, si le masquage *ex ante* ne bloquait l'accès à un commentaire que pour l'utilisateur ayant initié le blocage, l'utilisateur masqué ne pourrait pas connaître les caractères censurés à l'aide d'un deuxième compte et serait obligé, pour acquérir cette connaissance, d'obtenir les identifiants de l'utilisateur masqueur afin d'accéder à la liste des caractères censurés. **Un masquage *ex ante* qui ne s'impose qu'à l'initiateur ou à un nombre limité d'internautes renforce donc l'imprévisibilité des sources de masquage** : l'utilisateur dont les contenus sont masqués ignore qu'ils le sont, n'a alors aucune raison de contourner un blocage dont il ignore être l'objet, et peut d'ailleurs difficilement contourner. En imposant le masquage du contenu à tous les utilisateurs, **le masquage *ex ante* proposé par Instagram a donc pour premier inconvénient** de fournir à l'utilisateur dont les contenus sont masqués les moyens pour connaître facilement les caractères et suites de caractères censurés, donc **de faciliter le contournement** par rapport à un masquage *ex ante* ne s'imposant qu'à l'initiateur⁷⁰⁰.

Automatisé, **le masquage *ex ante* d'Instagram a pour deuxième inconvénient d'aggraver le risque de sur-blocage ou de sous-blocage**. On donne plusieurs exemples de messages haineux, facilement trouvés sur les réseaux sociaux : une jeune utilisatrice partage une vidéo sur Instagram, où on la voit intubée à l'hôpital, accompagnée de la légende « *les mecs qui balance de l'argent dans les snkrs [modèle de chaussures Nike] ca fait pitié* », et reçoit pour commentaire « *déjà faut rester en vie puis on verra* » ; une utilisatrice sans bras ni jambes s'expose en vidéo sur Snapchat, et reçoit pour commentaire « *on dirai le parfum de jean pol gotier* » ; un utilisateur de Twitter publie « *j'ai rien contre les tétraplégiques mais c'est un mot bien long pour peu de capacités* » etc. Dans ces trois commentaires, on voit mal les mots qui

699HERMANN Vincent, « Instagram autorise le blocage de mots-clés dans les commentaires », *NextInPact*, sept. 2016

700Précisons toutefois que, initié par des utilisateurs, le masquage proposé par Instagram sera toujours plus difficile à contourner qu'un masquage initié par l'application en démultipliant les sources de masquage

pourraient être censurés sans provoquer un sur-blocage, car l’injure ne découle pas des caractères employés mais de la signification des mots dans leur contexte d’utilisation⁷⁰¹.

Le deuxième cas qu’on étudie est le *Kids Only Safety Act*, un projet de loi fédérale aux États-Unis déposé au Sénat le 16 février 2022⁷⁰². Le KOSA exploite pleinement l’avantage du blocage dès les serveurs, à savoir l’établissement de cloisons entre des espaces logiques. Précisément, ce projet de loi entend cloisonner certains espaces logiques utilisés par les mineurs, dans le but d’exclure les majeurs de ces espaces réservés aux mineurs. À cette fin, le KOSA fixe trois catégories d’obligations pour les services, de toute taille, « *raisonnablement susceptible d’être utilisés* » par des enfants de 16 ans ou moins.

Premièrement, ces services doivent « *prévenir et atténuer les risques de dommages physiques, émotionnels, développementaux ou matériels causés* » par la promotion de l’automutilation, du suicide, des troubles alimentaires, de la toxicomanie, des « *questions qui présentent un risque pour la santé physique et mentale* » de l’enfant de 16 ans ou moins, de l’intimidation en ligne, du harcèlement d’un mineur de 16 ans, de l’exploitation sexuelle (incitation, grooming⁷⁰³ ou traite à des fins sexuels, abus sexuels de mineurs, trafic de matériel pédopornographique en ligne...), de la promotion et la commercialisation de produits ou services illicites pour les mineurs de 16 ans (drogues illicites, tabac, jeux d’argent, alcool...), et des pratiques commerciales prédatrices, déloyales ou trompeuses⁷⁰⁴. Deuxièmement, ces services doivent fournir aux parents des outils pour surveiller le temps passé par leurs enfants sur lesdits services, pour contrôler la confidentialité et les paramètres du compte de l’enfant, pour restreindre les possibilités d’achats et de transactions financières par l’enfant, pour contrôler la survenance des dommages listés par l’art. 3 (b), pour signaler au service des préjudices subis par un mineur, pour communiquer avec un point de contact électronique chargé des atteintes aux mineurs et pour suivre le traitement du signalement⁷⁰⁵. Troisièmement, ces services doivent fournir aux mineurs ou aux parents agissant pour le compte d’un mineur des outils clairs et visibles pour s’extraire des algorithmes de suggestion, pour restreindre les recommandations selon leur type ou catégorie, pour limiter les fonctionnalités qui incitent les mineurs à consacrer plus de temps aux services (telles les notifications, la lecture automatique, les récompenses pour le temps consacré...), pour restreindre le partage et le suivi de la géolocalisation d’un mineur, pour limiter la capacité des personnes n’ayant aucun lien avec le mineur à contacter un mineur ou à le trouver sur internet et pour empêcher les tiers de consulter ses données personnelles⁷⁰⁶.

À coups de bannissements (totaux ou partiels, initiés par l’application et par l’utilisateur mineur ou le parent contre les utilisateurs suspects) et de masquages *ex ante* des contenus (initié par l’application dans le cadre de son obligation de « *prévention* » et par l’utilisateur parent) voire de suppressions de données, le législateur américain espère enfermer les mineurs dans une bulle de protection vis-à-vis des utilisateurs et contenus préjudiciables aux mineurs. Ces méthodes ont pour avantages de

⁷⁰¹Ce défaut pourra plus tard être corrigé par l’intelligence artificielle, mais on verra que le recours à l’IA s’accompagne de nouveaux inconvénients

⁷⁰²Ce projet de loi vise à moderniser le COPPA (*Children’s Online Privacy Protection Rule*), une loi fédérale de 1998 qui protège les données personnelles des mineurs

⁷⁰³ Le grooming est une pratique par laquelle un majeur converse en ligne avec un mineur dans un but sexuel

⁷⁰⁴ *Kids Online Safety Act* (projet de loi), art. 3 (b)

⁷⁰⁵ *Ibid.*, art. 4 (b) et (c)

⁷⁰⁶ *Ibid.*, art. 4 (a)

pouvoir cibler à la fois les utilisateurs et les contenus illicites (bannissement et masquage), de couvrir tous les utilisateurs et contenus illicites et pas seulement les utilisateurs et contenus indésirables (initiation du blocage par le service), d'empêcher l'accès à une partie ou à une totalité du service selon l'espace logique d'où provient le contenu ou l'utilisateur illicite, de démultiplier les sources de blocage (initiation du blocage par l'utilisateur parent ou mineur), de s'exercer sans menacer la liberté d'autrui d'utiliser le service (initiation du masquage par l'utilisateur parent ou mineur), et d'intervenir en amont de toute amplification de l'échelle de diffusion d'un contenu illicite (masquage *ex ante*).

Leur efficacité est toutefois relativisée par plusieurs inconvénients. Le premier est l'aggravation du risque de sur-blocage des contenus, en raison de l'automatisation du masquage *ex ante*. Par exemple, « *les publications décrivant les conditions d'utilisation du naxolone, un médicament capable d'inverser une surdose d'opioïdes pourrait être considéré comme favorisant l'automutilation* », alors que l'information aiderait un adolescent drogué à son insu ; de même, il n'existe pas à ce jour de moyens pour distinguer « *un contenu qui exacerbe un trouble de l'alimentation d'un contenu qui fournir des informations et des conseils de santé nécessaires sur le sujet* »⁷⁰⁷.

Le deuxième inconvénient du dispositif KOSA réside dans le fait qu'il facilite son contournement. Certes, ce dispositif démultiplie les sources de blocage (bannissement partiel et masquage *ex ante* initiés par les utilisateurs) pour opposer une certaine imprévisibilité aux tentatives de contournement. Ainsi, les utilisateurs suspects qui tenteront d'accéder aux comptes d'utilisateurs mineurs se heurteront effectivement aux différents choix de blocage faits individuellement par les parents et/ou leurs enfants. En sens inverse toutefois, les utilisateurs mineurs peuvent assez facilement contourner le blocage pour accéder à des utilisateurs ou contenus suspects. En effet, **lorsque la source de blocage est un parent, l'utilisateur mineur** qui se voit bloquer l'accès à un contenu ou à un autre utilisateur n'est pas confronté à une diversité de sources de blocage éparpillées, mais **à une seule source de blocage** – leur(s) parent(s). Le blocage par un parent de l'accès à un contenu ou à un utilisateur par son enfant réduit donc à la fois la diversité des sources de blocage pour l'enfant, mais aussi leur imprévisibilité car l'enfant connaît très bien ses parents humainement, sources de son blocage. En l'espèce, le contrôle parental s'applique au compte de l'utilisateur mineur connu par le parent. Pour s'en échapper, il suffit donc au mineur de créer un compte clandestin, méconnu des parents, contournant ainsi le système de blocage reposant sur une unique source de blocage (par ailleurs parentale, donc bien connue par l'enfant bloqué).

B) Le blocage par non-interopérabilité

On appelle « blocage par non-interopérabilité » la technique qui consiste à empêcher, dès les serveurs, l'accès à une application en rendant cette dernière non-interopérable avec un autre programme. Par exemple, la quasi-totalité des applications développées par Apple (AppStore, iCloud, iMessage, Safari, Siri, Apple Pay, FaceTime, Apple News...) sont non-interopérables avec d'autres systèmes d'exploitation que ceux d'Apple (macOS pour les ordinateurs Mac, iOS pour les iPhones, iPadOS pour les iPads...). Ou encore en Chine, vers 2011-2012, la messagerie instantanée QQ (appartenant à Tencent) s'était rendue volontairement non-interopérable avec le logiciel antivirus 360

⁷⁰⁷ KELLEY Jason et MACKEY Aaron, « KOSA Would Let the Government Control What Young People See Online » [en ligne], *Electronic Frontier Foundation*, nov. 2022 ; KELLEY J., MACKEY A., « Dangerous "Kids Online Safety Act" Does Not Belong in Must-Pass Legislation », *Electronic Frontier Foundation*, déc. 2022

Safeguard (appartenant à Qihoo)⁷⁰⁸. Les fonctions des deux applications étant incompatibles pour l'exécution de QQ, l'utilisateur équipé de cet antivirus ne pouvait utiliser par ailleurs QQ, l'obligeant ainsi à choisir entre utiliser 360 Safeguard ou utiliser QQ.

Dès lors, le blocage par lequel QQ empêche son accès aux utilisateurs de 360 Safeguard est conditionné, non par l'identité d'un internaute (bannissement par blocage), mais par l'utilisation d'un autre logiciel (blocage par non-interopérabilité). Or, dans la mesure où QQ couvrait à lui seul 80% du marché chinois des messageries instantanées en 2014, ce blocage privait la majorité des internautes chinois du droit d'utiliser simultanément QQ et 360 Safeguard. Cette pratique anticoncurrentielle dite du « choisir l'un ou l'autre » (*choose one from two*) a conduit Qihoo à porter plainte contre Tencent, dénonçant une violation de l'ancien article 17 (4) de la Loi chinoise Anti-Monopole (désormais art. 22) qui interdit aux entreprises en position dominante sur le marché chinois « *de permettre, sans motif valable, à leurs homologues commerciaux d'effectuer des transactions exclusivement avec elles-mêmes ou avec les entreprises qu'elles désignent* ».

La Cour populaire suprême chinoise reconnaît que le blocage effectué par Tencent relève d'une pratique anticoncurrentielle en qualité d' « incompatibilités de produits », mais déboute Qihoo de sa demande, aux motifs que Tencent n'est pas en situation de position dominante sur son segment de marché (réseaux sociaux et services de messagerie)⁷⁰⁹. Malgré sa part de marché – un « *indicateur relativement grossier et potentiellement trompeur de la position dominante sur le marché* » selon la Cour –, Tencent n'a pas le pouvoir de fixer les conditions de concurrence sur son segment de marché, ni celui de contrôler les prix, le volume ou les transactions réalisées sur ce marché ; les concurrents ne sont pas excessivement dépendants à l'égard de Tencent pour leurs transactions, et ne sont pas non plus excessivement empêchés par Tencent d'accéder au segment de marché pertinent⁷¹⁰. Faute de position dominante, poursuit la Cour, l'incompatibilité « *n'a pas eu pour effet évident d'éliminer ou de restreindre la concurrence* » sur le segment de marché pertinent, dont l'antivirus 360 Safeguard ne fait d'ailleurs pas partie. En d'autres termes, le blocage par non-interopérabilité n'est pas contraire au droit chinois de la concurrence s'il est mené par une application contre une application issue d'un autre segment de marché.

Le blocage par non-interopérabilité est adapté lorsque la R-DATA provient, non d'un utilisateur ou d'un contenu, mais d'un logiciel (voire de plusieurs logiciels qui comportent un même script non interopérable avec le logiciel bloqueur). En plus d'être la seule technique de blocage à pouvoir cibler un logiciel, cette technique a pour deuxième avantage d'être très difficilement incontournable : l'impossibilité d'exécuter les tâches de deux logiciels différents durera aussi longtemps que le propriétaire de l'application ne corrige pas le défaut d'interopérabilité.

Un tel blocage a toutefois d'importants inconvénients. D'abord, il n'est adapté que contre un logiciel dont le logiciel bloqueur connaît les scripts (ce qui rend cette technique très peu utile contre les logiciels malveillants encore inconnus, trop nombreux et diversifiés par leur code source). Ensuite, le

⁷⁰⁸ WANG Jing, « Sustainability of China's anti-monopoly law in the digital era: an observation on the 'choosing one from two' jurisprudence from China », Paper presented at 19th Asian Law Institute Conference, Tokyo, Japan, 2022

⁷⁰⁹ 奇虎公司与腾讯公司垄断纠纷上诉案 [Qihoo 360 v. Tencent], 2013 SUP. PEOPLE'S CHINA CIVIL JUDGMENT No. Minsanzhongzi 4/2013

⁷¹⁰ Ibid., point II du jugement

blocage par non-interopérabilité impose à l'utilisateur de faire un choix entre l'application bloqueuse et les programmes bloqués, mais il ne garantit pas toujours que l'utilisateur choisira l'application bloqueuse au détriment des programmes bloqués. Surtout, un manque d'interopérabilité peut avoir des conséquences de plus en plus graves compte tenu de l'intégration croissante des technologies de réseau dans l'organisation sociale. Un défaut d'interopérabilité entre les messageries instantanées (WhatsApp, Signal, Messenger...) et/ou les services de stockage de fichiers en cloud (Google Drive, OneDrive, iCloud...) compliquera lourdement la communication au sein d'une entreprise, d'une administration ou d'un établissement de santé si les employés et agents utilisent des messageries instantanées ou des services de stockage cloud différents ; un défaut d'interopérabilité entre les messageries instantanées et les logiciels antivirus, ou entre les navigateurs web et les VPN fragiliserait considérablement la sécurité des informations hébergées par des entreprises, des administrations ou des établissements de santé en les privant de l'utilisation d'un antivirus ou du pouvoir de chiffrer leur connexion ; un défaut d'interopérabilité entre les différents systèmes d'exploitation utilisés et les bases de données peut bouleverser l'organisation d'une entreprise (incapable d'accéder correctement aux comptes clients, aux factures et à la comptabilité, aux informations sur la fourniture et l'approvisionnement...), d'une administration ou d'un établissement de santé (incapable d'accéder ou de transférer correctement les informations relatives aux patients) etc. On en déduit que le blocage par interopérabilité doit être limité le plus possible, aux seuls cas où le logiciel bloqué est avéré dangereux.

Paragraphe 3 – La désactivation de fonctions logicielles par blocage

A déjà été examinée l'hypothèse du blocage d'un logiciel dans son entier. On s'intéressera ici au blocage de *certaines* fonctions logicielles seulement, à travers le cas du blocage opéré en Russie pour certaines fonctions de TikTok (A), dont on évaluera l'efficacité pour préserver la souveraineté numérique de la Russie (B).

A) Étude de cas : l'efficacité du blocage de fonctions par TikTok en Russie

1. Présentation de la technique de désactivation de fonctions par blocage

Le stockage d'une R-DATA peut ensuite être bloqué par désactivation d'une ou plusieurs fonctions d'une application. On a vu qu'une fonction peut être désactivée *par suppression de données*, auquel cas les données qui correspondent à cette fonction sont éliminées de l'espace mémoire des serveurs hébergeant ladite fonction. Une fonction peut aussi être désactivée *par blocage de données*, auquel cas les données qui correspondent à cette fonction sont toujours présentes dans l'espace mémoire des serveurs, mais leur accessibilité est empêchée. C'est le cas qui nous occupe ici. La nuance est importante car ces deux façons de désactiver une fonction se contournent différemment : la suppression d'une fonction depuis un serveur peut être contournée en reproduisant la même fonction sur un autre serveur ; le blocage d'une fonction depuis un serveur peut être contourné en trouvant un moyen d'accéder à la fonction toujours hébergée par ce même serveur.

Que la fonction soit désactivée par suppression ou par blocage, la désactivation apporte le même avantage : désactiver une fonction revient à priver l'internaute du pouvoir de faire exécuter cette fonction. **En privant l'utilisateur d'une capacité d'action, cette technique permet donc de lui retirer le pouvoir de faire réaliser la R-DATA qui découle de la fonction bloquée.** La désactivation d'une fonction ne permet donc pas de cibler une destination,

un contenu, un utilisateur ou un programme mais une capacité d'action de l'utilisateur. **La désactivation par blocage** apporte par ailleurs un fort avantage sur la désactivation par suppression : elle **permet de réserver l'usage d'une fonction à une catégorie d'utilisateurs**. Cet avantage est particulièrement utile pour réserver aux modérateurs certaines fonctions de modération (bannissement d'un utilisateur, suppression ou masquage de contenus...).

En revanche, **la désactivation d'une fonction par blocage** partage le même inconvénient que la désactivation par suppression : elle **n'est adaptée que si la R-DATA provient essentiellement de la fonction désactivée**. Si au contraire la R-DATA peut être largement produite et diffusée à l'aide d'autres fonctions que celle désactivée, la désactivation se montrera peu efficace ou inefficace pour réduire l'échelle de diffusion de cette R-DATA. Elle se montrera même contreproductive si la R-DATA peut provenir de fonctions indispensables au service (fonctions d'envoi de messages privés, de publication de commentaires, de partage d'images ou de vidéos...), car la désactivation d'une fonction indispensable peut diminuer la qualité et l'utilité d'une application auprès des utilisateurs, donc engendrer des migrations des utilisateurs et de la R-DATA vers d'autres applications.

La désactivation d'une fonction par blocage a par ailleurs pour deuxième inconvénient de **faciliter le contournement** par rapport à la désactivation par suppression. En effet, la suppression d'une fonction suppose son élimination de l'espace mémoire du serveur. Elle ne peut donc être contournée qu'en reproduisant sur un serveur la même fonction dans le cadre d'une autre application (par ex., un utilisateur peut publier des vidéos courtes sur Instagram ou YouTube Shorts si TikTok supprime la fonction de publication de vidéos), ou dans le cadre d'une extension logicielle (*plug-in*). Une extension logicielle est un programme (par exemple un bloqueur de publicités) qui complète une application principale (par exemple un navigateur web), susceptible d'être créée aussi bien par le propriétaire de l'application principale que par n'importe quel programmeur tiers. Par exemple, Facebook s'est toujours refusé à proposer la fonction « dislike » (« je n'aime pas ») vis-à-vis d'un contenu. Au début des années 2010, plusieurs tiers ont alors proposé le téléchargement de plug-in (di.liik.es, Facebook Dislike, Dislike Button de WebGoggles...) qui offrent aux utilisateurs de Facebook la fonction « dislike » – le dislike apposé sur un contenu ne s'affichera alors que pour l'utilisateur qui y a recouru et pour tous les utilisateurs qui ont téléchargé la même extension logicielle ⁷¹¹. Lorsqu'une fonction supprimée (ou jamais activée) par une application est produite par un plug-in, l'auteur du plug-in doit toutefois connaître le code source nécessaire pour que son programme soit interopérable avec l'application principale, et doit par ailleurs posséder des capacités d'hébergement à la mesure des services proposés par son plug-in⁷¹². *A contrario*, dans le cas de la désactivation par blocage, il n'est pas nécessaire de programmer une application interopérable avec l'application concernée, ni même de produire ou reproduire la fonction. En cas de blocage, la fonction n'est pas supprimée. Elle reste hébergée sur le serveur, et il suffit donc de trouver un moyen d'accéder à des données déjà hébergées sur des serveurs. Ne nécessitant pas de rechercher une solution pour (re)produire et héberger la fonction, la désactivation d'une fonction par blocage facilite donc le contournement.

⁷¹¹ SMARTY Ann, « 2 Ways to DISlike Things on Facebook (FireFox and Google Chrome) », sur *Searchonlinejournal.com*, 16 juil. 2010 ; MANSUR Rachel, « How To Add A "Dislike" Button To Your Facebook Page », sur *Businessinsider.com*, 14 avr. 2011

⁷¹² Par exemple, il ne pourra pas ajouter à une application principale une fonction de publication de vidéos sans exploiter (donc payer) les serveurs d'hébergement nécessaires au stockage de toutes les vidéos des utilisateurs qui utilisent le plugin

On applique notre analyse sur la désactivation par blocage au cas concret de TikTok en Russie. On a relevé que, dans le cadre de la guerre russo-ukrainienne, TikTok a désactivé la fonction de publication de nouvelles vidéos pour ses utilisateurs russes, les privant ainsi du pouvoir de diffuser sur le réseau social de nouvelles vidéos susceptibles de contenir des fausses informations au sens de la loi russe. Plus précisément, TikTok n'a pas bloqué la fonction de publication mais la fonction de téléversement de nouvelles vidéos ⁷¹³. La fonction de téléversement restait hébergée sur les serveurs de TikTok mais elle était indisponible aux utilisateurs russes (du fait de leur géolocalisation). Tracking Exposed révèle que, dès les premières minutes qui ont suivi cette mesure, des influenceurs russes propagandistes ont contourné ce blocage pour téléverser sur TikTok des vidéos favorables au Kremlin⁷¹⁴, et une enquête journalistique de Vice rapporte que ces influenceurs ont été payés à cette fin (on ignore la source de ce financement)⁷¹⁵. Par ailleurs, plusieurs observateurs ont constaté que l'algorithme de TikTok privilégiait très nettement les vidéos prorusses lorsqu'étaient recherchés certains mots sur le réseau social comme le mot « ukrainie »⁷¹⁶. La technique ici mobilisée ne vise pas à bloquer mais à valoriser l'accès à des données – technique qu'on approfondira plus loin.

En moins d'un mois, TikTok qui constituait jusqu'alors une « *menace sérieuse pour le soutien national à la guerre* » est devenu un outil de propagande pro-Kremlin, un réseau social où seules sont tolérées les vidéos publiées par les propagandistes et les médias accrédités par la Fédération (RT, Sputnik, Ria Novosti...), auprès d'utilisateurs interdits de diffuser leurs propres vidéos ou d'accéder aux contenus étrangers, seulement autorisés à publier des commentaires, envoyer des messages, visualiser ou relayer les vidéos disponibles⁷¹⁷. Pour obtenir ce résultat, TikTok a donc combiné trois techniques de régulation : un blocage des contenus étrangers par

⁷¹³ Le téléversement désigne le transfert de fichiers (vidéos en l'espèce) depuis le client (application mobile de TikTok ou navigateur web pour accéder à TikTok sur ordinateur) vers le serveur (serveur hébergeant TikTok). Inversement, le téléchargement désigne le transfert de fichiers depuis le serveur vers le client.

⁷¹⁴ Le blocage a d'abord pu être contourné en accédant à TikTok non pas depuis l'application mobile mais depuis un navigateur web. TikTok a rapidement corrigé cette faille, et les internautes s'en sont saisi d'une deuxième. Toujours en accédant à TikTok depuis un navigateur web, le contournement a cette fois consisté à utiliser une adresse IP située en Russie depuis un VPN, puis à quitter le réseau russe en utilisant un autre VPN, à sélectionner et à téléverser le fichier que l'internaute désire publier, et enfin à changer de nouveau la localisation pour revenir sur le territoire russe avant de cliquer sur « post » pour publier la vidéo. V. « Content Restrictions on TikTok in Russia following the Ukrainian War », sur *Tracking.exposed* [association de chercheurs], 13 avr. 2022

⁷¹⁵ Les influenceurs s'organisaient sur un canal privé (groupe de discussion accessible uniquement sur invitation) de la messagerie instantanée Telegram. L'administrateur du groupe, avec lequel s'est entretenue l'équipe de Vice, communiquait aux 500 membres du canal : les étapes à suivre pour contourner l'interdiction de publication de vidéos sur TikTok ; certains mots, hashtags voire phrases que doivent employer les influenceurs ; les lieux de tournage sur lesquels les influenceurs doivent capturer leurs vidéos ; la date et l'heure auxquelles ils doivent publier. Il semble que les sommes d'argent – dont on ignore le montant – versées en contrepartie aux influenceurs étaient aussi conditionnées par le nombre de « vues » que récoltait une vidéo. GILBERT David, « Russian TikTok Influencers Are Being Paid to Spread Kremlin Propaganda », sur *Vice.com*, 11 mars 2022

⁷¹⁶ CROQUET Pauline, « TikTok coupe la Russie du reste du monde en bloquant les contenus étrangers » [en ligne], *Le Monde*, 10 mars 2022

⁷¹⁷ OREMUS Will, « TikTok created an alternate universe just for Russia », sur *Washingtonpost.com*, 13 avr. 2022

géolocalisation ; un blocage de la fonction de téléversement de vidéos ; et une surexposition des vidéos propagandistes.

On se concentre ici sur la technique du blocage de la fonction de téléversement de vidéos. On a vu que la désactivation d'une fonction par blocage a pour avantage de réserver l'usage de cette fonction à une catégorie d'utilisateurs. En l'espèce, le blocage décidé par TikTok était donc une technique adaptée pour garder la fonction disponible aux utilisateurs résidant hors de Russie, tout en la rendant indisponible aux utilisateurs résidant en Russie. On a vu aussi que le recours au blocage pour désactiver une fonction a pour inconvénient de n'être approprié que si la R-DATA découle essentiellement de la fonction désactivée. En l'espèce, TikTok étant précisément un réseau social de partage de courtes vidéos, le téléversement de vidéos est le principal outil susceptible de diffuser largement sur TikTok des fausses informations au sens de la loi russe. Les utilisateurs pourraient être tentés de diffuser de fausses informations dans l'espace commentaires situé en-dessous des vidéos, mais la loi russe les en dissuade lourdement en menaçant les auteurs de fausses informations sur l'armée d'une très lourde peine de 10 à 15 ans d'emprisonnement. Dès lors, soutenu par la dissuasion pénale, le blocage mené par TikTok évite largement la diffusion de fausses informations en privant les utilisateurs de leur principale capacité pour diffuser de tels contenus illicites sur TikTok.

Le blocage de la fonction de téléversement par TikTok semble donc profiter des avantages de la désactivation d'une fonction par blocage, tout en s'épargnant les inconvénients. Il est toutefois rattrapé par le deuxième inconvénient de la désactivation par blocage, à savoir la facilitation du contournement. En effet, la fonction n'est pas supprimée ; elle est toujours hébergée sur les serveurs exploités par TikTok, donc accessible d'une manière ou d'une autre. Le blocage est ici géolocalisé, donc la fonction bloquée est accessible pour les espaces géographiques hors Russie. L'utilisateur peut alors simplement contourner le blocage en empruntant une adresse IP située en-dehors de la Russie.

On a vu que les propagandistes ont exploité cette faille en alternant l'utilisation de deux VPN. On doute cependant qu'ils soient les seuls à l'avoir exploitée. Sur YouTube, publiée en juin 2022, la vidéo russe « Contourner TikTok en Russie en 30 secondes ! » cumule 1,1 millions de vues en mars 2023 ; sur le réseau social russe vc.ru, l'article « Comment contourner les blocages de TikTok en Russie » a été vu 1,09 millions de fois en mars 2023 ; sur le blog collaboratif Habr, l'article de blog « comment contourner le blocage de TikTok en Russie » totalise 308 000 vues à la même date ; lorsqu'on recherche « Как обойти блокировку TikTok » (comment contourner TikTok) sur le moteur de recherche Yandex, le premier résultat proposé est « Comment contourner le blocage de TikTok en 2023, TOP VPN pour TikTok »⁷¹⁸ etc. « *Le nombre de téléchargements quotidiens en Russie pour les 10 VPN les plus populaires est passé de 15 000 avant la guerre à 475 000 en mars [2022], et se sont poursuivis à un rythme de près de 300 000 par jour [le 7 mai 2022]* »⁷¹⁹.

⁷¹⁸ « ВОСКРЕСИЛ Tik Tok в России за 30 сек.! | Как обойти блокировку тик ток и как выложить видео в 2022? », sur *Youtube.com*, juin 2022 ; « Как обойти блокировки TikTok в России », sur *Vc.ru*, 28 juin 2022 [consulté le 30 mars 2023] ; « Как обойти блокировку TikTok в России », sur *Habr.com*, 8 mars 2022 ; « Как обойти блокировку Тик-Ток в 2023 году, ТОП VPN для Tik-Tok'a », sur *Gruzddev.ru*, 28 avril 2023

⁷¹⁹ « VPN use skyrockets in Russia during Ukraine invasion », sur *Aljazeera.com*, 7 mai 2022

Le blocage mené par TikTok ne se soustrait pas au troisième inconvénient de la désactivation d'une fonction : l'aggravation du risque de sur-blocage. De nombreuses entreprises qui promouvaient leurs produits et services sur TikTok, ainsi que la plupart des influenceurs russes qui exerçaient leur métier sur TikTok, ont perdu leurs revenus ou se sont retrouvés obligés de migrer vers d'autres plateformes⁷²⁰. Pour ceux d'entre eux qui ont migré, les entreprises et influenceurs russes semblent s'être principalement orientés vers les réseaux sociaux VKontakte (et son application de courtes vidéos VK Clips), Telegram, Yandex Zen, YouTube, Pinterest et Instagram⁷²¹.

1. L'efficacité de la régulation de TikTok en Russie pour empêcher l'accès aux informations étrangères et l'opposition au gouvernement

In fine, les techniques de restriction mises en œuvre en Russie après l'invasion russe de février 2022 en Ukraine ont-elles été efficaces ? Les techniques ici étudiées sont le blocage initié par TikTok (désactivation de la fonction de téléversement de vidéos pour les utilisateurs russes, et blocage de l'accès aux comptes et contenus étrangers) ainsi que le blocage dès l'acheminement par les FAI russes sur ordre du Roskomnadzor contre Messenger, Twitter et Quora par moments, Instagram, Facebook, SoundCloud, le jeu d'échecs en ligne [Chess.com](https://chess.com), BBC, Google News, Radio Free Europe, The Telegraph, NPR, Deutsche Welle, et les principaux médias finlandais Ilta-Sanomat, Helsingin Sanomat et l'Yle, la quasi-totalité des médias russes indépendants (Meduza, Agentstvo, [Snob.ru](https://snob.ru), [Republic.ru](https://republic.ru), Mediazona...) etc. ⁷²² Telle qu'on l'a définie, l'efficacité de la régulation dépend de l'objectif recherché par le régulateur.

Si la Fédération de Russie avait pour objectif d'**empêcher TikTok de devenir un canal d'opposition à la guerre, la régulation initiée par TikTok nous semble avoir été efficace**. En effet, les témoignages et enquêtes journalistiques qu'on a croisés rapportent l'existence d'une « ville fantôme », un réseau social réduit à une application d'archivage sur laquelle subsistent des propagandistes survalorisés par rapport à l'adhésion qu'ils suscitent, et quelques influenceurs de divertissement qui contournent le blocage⁷²³.

Si la Fédération de Russie avait pour objectif d'**empêcher l'opposition à la guerre sur le réseau internet russe, le succès de la régulation est plus mitigé**. En effet, l'opposition à la guerre ne nous semble pas massive sur le territoire russe, et paraît surtout dispersée. D'une part,

⁷²⁰ SHIGAREVA Margarita, « "Certains sont simplement retournés à la besogne" Comment la vie des blogueurs russes a-t-elle changé en un an sans TikTok ? » («Некоторые просто в шарагу пошли обратно» Как изменилась жизнь российских блогеров за год без TikTok?), sur *Lenta.ru* [journal d'État], 9 mars 2023

⁷²¹ KASHEVSKY Valery, « La Russie a-t-elle réussi à créer un substitut aux réseaux sociaux étrangers ? » (Получилось ли у России создать замену иностранным соцсетям?), sur *Eurasianet.org*, 1^{er} déc. 2022. Eurasianet est un organe de presse indépendant qui couvre les régions du Caucase du Sud et de l'Asie centrale.

⁷²² « Russia Has Blocked 138K Websites Since Ukraine Invasion, Prosecutor Says », *The Moscow Times*, 8 août 2022 ; « A list of all websites and platforms blocked in Russia », sur *Purevpn.com*, 5 janv. 2023 ; MIGLIANO Simon et WOODHAMS Samuel, « Websites Blocked in Russia Since Ukraine Invasion », sur *Top10vpn.com*, 27 janv. 2023

⁷²³ OREMUS W., « TikTok created an alternate universe just for Russia », préc., *Washington Post*, 2022 ; FEDOROVA Maria, « Tiktoker universel. Ce que font les blogueurs six mois après le blocage de l'application TikTok en Russie » (Универсальный тиктокер. Чем занимаются блогеры спустя полгода после блокировки приложения TikTok в России), *Nasha Versia* (média russe indépendant), 5 nov. 2022

une grande partie des opposants russes à la guerre a émigré – plus de 700 000 russes ont quitté le territoire entre janvier et octobre 2022 par opposition à la guerre, par difficultés économiques face aux sanctions occidentales ou par crainte d'être mobilisée⁷²⁴. D'autre part, il semble que la majorité de la population russe soutienne la guerre. Cependant, ce résultat s'explique moins par les techniques de restriction déployées sur internet que par la propagande menée par le Kremlin : le média le plus populaire en Russie – la télévision – est contrôlé par l'État russe, tout comme la radio et la presse⁷²⁵ ; le ministère de la Défense mène depuis 2009, auprès de la jeunesse, une campagne patriotique axée sur la puissance militaire russe (pour le recrutement et l'amélioration de l'image de l'armée fédérale)⁷²⁶ ; et, pour ce qui est d'internet, le Kremlin a réservé des fonds publics à l'instauration de « TikTok houses » – des salles de classe dans les établissements d'enseignement supérieurs qui accueillent des adolescents et jeunes adultes pour diffuser des contenus de propagande sur TikTok⁷²⁷. Dès lors, pour ce qui est d'internet, l'adhésion de la population aux raisons d'être de la guerre est imputable à des techniques d'augmentation de l'accès à des contenus (propagandistes) davantage qu'à des techniques de restriction des contenus comme le détaillera plus loin.

Entre l'exil des opposants et la propagande fédérale, le soutien de la population russe à la guerre est certes vaste, mais fragile. Le soutien populaire est fragile, d'abord parce que ce soutien prend assez peu la forme d'une adhésion à la guerre mais plutôt d'une absence de résistance. Pour le sociologue russe Lev Goudkov, directeur scientifique de l'institut Levada, *« il y a 270 des médias les plus populaires qui ont été bloqués. Même s'il existe des possibilités d'information alternatives, la grande masse des gens n'en veut pas. Ça les maintient dans un état psychologique confortable : 'Je ne sais rien, ne me dites pas de choses désagréables. 'On*

⁷²⁴ TOFANYUK Elena et SAPRONOVA Ioulia, « Quelque 700 000 citoyens ont quitté la Russie depuis le 21 septembre » (Россию после 21 сентября покинули около 700 000 граждан), sur *Forbes.ru*, 4 oct. 2022

⁷²⁵ Une enquête d'opinions menée en mars 2023 par des sociologues russes du Centre de recherche Levada confirme que la télévision demeure le média le plus populaire en Russie : à la question « où vous informez-vous le plus souvent sur l'actualité du pays et du monde ? » (Откуда Вы чаще всего узнаете о новостях в стране и мире?), 64% des répondants désignent la télévision (contre 88% en août 2013, 74% en septembre 2018, 69% en août 2020 et 61% en décembre 2021). 41% des répondants désignent les réseaux sociaux sur internet (contre 14% en août 2013, 29% en septembre 2018, 39% en août 2020 et 40% en décembre 2021), et 33% désignent les éditions en ligne (contre 21% en août 2013, 37% en septembre 2018, 38% en août 2020 et 31% en décembre 2021). Sur ces résultats, v. « Principales sources d'information et journalistes populaires » (Основные источники информации и популярные журналисты), sur *Levada.ru*, avr. 2023. Concernant le contrôle des médias par la Fédération de Russie, v. CHUPIN Ivan, « Des médias aux ordres de Poutine ? », *Savoir/Agir*, n° 28 2014, p. 33-38 ; ZAKHAROVA Maria et PAUTHE Nicolas, « La liberté de la presse et des médias en Russie », *Droit et Société*, n° 93, 2016, p. 437-452 ; CHUPIN Ivan et MUSTAFINA Renata, « Quand le geste révèle le militant : sur quelques cas d'entrée en journalisme d'opposition dans la Russie contemporaine », *Critique Internationale*, n°79, 2018, p. 159-179 ; v. aussi le mémoire de maîtrise de HOPSTAD Birgitte, « The Russian media under Putin and Medvedev: Controlled media in an authoritarian system », sur *Ntnuopen.ntnu.no* [Université norvégienne des sciences et de technologie, NTNU], 2011

⁷²⁶ KASTOUÉVA-JEAN Tatiana, « L'éducation patriotique et militaire, un avatar de l'époque soviétique ? », *Revue Défense Nationale*, n° 802, 2017, p. 72-77

⁷²⁷ PANKRATOVA Irina, « Guerre et paix dans TikTok. Comment les "maisons tiktok" russes se sont transformées en bureaux de propagande militaire » (« Война и мир в TikTok. Как российские «ТИКТОК-ХАУСЫ» превратились в офисы военной пропаганды »), sur *Thebell.io*, 22 juil. 2022

peut dire en effet que c'est une protection. »⁷²⁸. Le soutien populaire est fragile, ensuite parce qu'il est divisé entre les générations et entre les régions. Les Russes âgés de plus de 40 ans et ceux vivant dans les banlieues et villages s'informent principalement par la télévision et la radio, tandis que les Russes âgés de moins de 35 ans et ceux habitant les grandes villes s'informent davantage par internet⁷²⁹. Or, 35% des jeunes russes s'opposent clairement à la guerre, provoquant des conflits intergénérationnels sur le sujet de la guerre en Ukraine entre les enfants russes et leurs parents qui reprennent l'argument gouvernemental de la « dénazification » de l'Ukraine⁷³⁰. De même, tout au long de l'année 2022, on observe une « fuite des cerveaux » depuis la Russie, une émigration intense qui touche principalement les ingénieurs, chercheurs, programmeurs et cadres du secteur technologique...⁷³¹ L'exode du secteur technologique est si nuisible à la Russie que le gouvernement russe a d'abord recruté des informaticiens talentueux dans les prisons russes en mai 2022, puis s'est résigné à multiplier les exemptions de mobilisation dont peuvent bénéficier les informaticiens exilés⁷³². **La fragilité du soutien populaire russe à la guerre a donc de graves conséquences sur l'unité intrafamiliale** (conflits intergénérationnels), **et sur le développement technologique de la Russie**⁷³³. Ces données suggèrent que la **régulation d'internet pratiquée par la Russie n'a été que très relativement efficace auprès des jeunes générations et des habitants des grandes villes pour empêcher leur opposition à la guerre.**

Si la Fédération de Russie avait pour objectif d'**empêcher l'accès de la population russe aux informations étrangères traitant de la guerre en Ukraine**, la régulation d'internet pratiquée par la Russie nous semble avoir une **efficacité là encore très relative**. D'un côté, TikTok a pour particularité de soumettre à l'utilisateur des vidéos qu'il n'a pas préalablement choisies de visualiser. De cette façon, on pense que le blocage de contenus étrangers sur TikTok a été efficace pour réduire la consultation accidentelle de contenus étrangers par les utilisateurs russes. D'un autre côté, les restrictions mises en œuvre par la Russie n'ont que très limitativement efficace pour réduire la consultation intentionnelle de contenus étrangers. D'abord, les blocages dès l'acheminement de la presse étrangère et indépendante n'empêchent pas les médias bloqués de conserver, un an après leur blocage, la moitié voire les trois quarts

728 « "Nous sommes fiers de notre armée" : la population russe soutient-elle vraiment la guerre en Ukraine ? », *France Info*, 18 fév. 2023

729 L'enquête d'opinions précitée du Centre Levada rapporte que, en mars 2023, 95% des 18-24 ans se connectent quotidiennement ou quasi-quotidiennement à internet en Russie, contre 73% des 40-54 ans et 44% des 55 ans et plus. Par ailleurs, 91% des répondants de 18 à 24 ans accèdent quotidiennement à des réseaux sociaux, contre 30% pour les 55 ans et plus. V. « Principales sources d'information et journalistes populaires » (Основные источники информации и популярные журналисты), sur *Levada.ru*, avr. 2023.

730 « "Nous sommes fiers de notre armée" », préc., *France Info*, 2023

731 « En Russie, le secteur technologique subit un exode sans précédent », *Courrier International*, 2 mai 2022 ; L'HOSPITAL Alix, « Fuite des cerveaux : "La Russie ne dispose pas d'un vivier de talents pour les remplacer" », *L'Express*, 27 mai 2022 ; PINNA Monica, « L'exode silencieux des élites culturelles de Russie suite à la guerre en Ukraine », *Euronews*, 21 déc. 2022

732 TOUZANI Samir, « La Russie déplore la fuite de 100.000 employés de la tech », *Les Echos*, 20 déc. 2022 ; « Face à l'exode des cerveaux, la Russie cherche des informaticiens doués en prison, selon un rapport », sur *Devellopez.com*, 5 mai 2022 ; TRONCHET Sylvain, « Guerre en Ukraine : la fuite des cerveaux a un impact sur le secteur de la "tech" russe », *France Info*, 23 janv. 2023

733 LEVRESSE Estelle, « Dmitri Orechkine, analyste politique: "La guerre en Ukraine n'unit pas la société russe. Elle la divise" », *L'Echo*, 29 mars 2022

de l'audience russe qu'ils possédaient avant leur blocage : on a vu que le nombre de visiteurs mensuels russes de la BBC est passé de 12-15 millions en février 2022 à 4,5-6 millions en mars 2023, et que celui de Meduza est passé 6-7 millions à 4-5 millions sur la même période. Dès lors, en mars 2023, une voire plusieurs dizaines de millions de russes continuent d'accéder chaque mois à la presse étrangère et indépendante, malgré son blocage dès l'acheminement. Ensuite, le blocage initié par TikTok n'a pas empêché les internautes russes d'accéder à des vidéos étrangères sur YouTube, qui totalisait plus de 90 millions d'utilisateurs actifs en Russie fin 2022⁷³⁴. comme l'illustrent les migrations d'influenceurs russes vers Instagram, le blocage initié par TikTok a motivé de nombreux utilisateurs à contourner le blocage d'Instagram par les FAI russes – on a vu que, en novembre 2022, 26 millions d'utilisateurs russes contournaient chaque mois le blocage d'Instagram dès l'acheminement. Par conséquent, si les restrictions ont sans doute largement limité la consultation accidentelle d'informations étrangères par les Russes sur internet, elles ont été assez inefficaces pour empêcher des dizaines de millions de Russes d'accéder intentionnellement à des informations étrangères.

Si la Fédération de Russie avait pour objectif d'**empêcher l'accès de la population russe à des informations exposant les échecs de l'armée russe**, les techniques de restriction déployées ont été **inefficaces**. En effet, les Russes ont largement connaissance des défaites et maladroites de l'armée russe en consultant, non seulement des informations étrangères, mais surtout des informations russes. Plusieurs influenceurs nationalistes russes, pro-guerre, entretiennent des contacts sur les lignes de front – comme Igor Girkin, ancien colonel du renseignement russe dont le compte Telegram @strelkovii cumulait 430 000 abonnés en septembre 2022 puis 794 000 en avril 2023, ou encore Starshe Eddy dont le compte Telegram @vysokygovorit totalisait 28 000 abonnés en janvier 2022, puis 500 000 en septembre 2022 et 625 000 en avril 2023⁷³⁵. Au près de leurs centaines de milliers d'abonnés, ils relaient les revers et humiliations de l'armée russe pour dénoncer l'inaction du Kremlin face aux défaites : « *la guerre en Ukraine continuera jusqu'à la défaite complète de la Russie* » pour Girkin, « *il faut dire qu'à Balakliia, les forces armées ukrainiennes ont complètement dépassé notre commandement* » pour Starshe Eddy, « *nous devons commencer à faire quelque chose à propos du système dans lequel nos dirigeants n'aiment pas parler des mauvaises nouvelles, et leurs subordonnés ne veulent pas contrarier leurs patrons* » publie sur Telegram le journaliste de guerre pro-Kremlin Aleksandr Kots qui comptait 658 000 abonnés en mars 2023⁷³⁶...

Si la Fédération de Russie avait pour objectif d'**empêcher l'opposition au gouvernement fédéral**, la régulation appliquée par la Russie a été **inefficace**. Depuis septembre 2022, les influenceurs russes d'extrême droite multiplient les appels à la mobilisation générale et à la démission – voire à la mise à mort – du ministre de la Défense, Sergueï Choïgou⁷³⁷. Comme le souligne le chercheur Pavel Luzin, politologue spécialisé dans la politique et les affaires militaires russes : les Russes ont besoin d'exprimer leur déception face aux défaites contre

⁷³⁴ KASHEVSKY Valery, « La Russie a-t-elle réussi à créer un substitut aux réseaux sociaux étrangers ? », préc., sur *Eurasianet.org*, 2022

⁷³⁵ SAUER Pjotr, « 'We have already lost': far-right Russian bloggers slam military failures », *The Guardian*, 8 sept. 2022

⁷³⁶ *Ibid.* et BEARDSWORTH James, « Explainer: Who Are Russia's Pro-War Bloggers And Why Are They Important? », *The Moscow Times*, 15 sept. 2022

⁷³⁷ BEARDSWORTH J., « Explainer: Who Are Russia's Pro-War Bloggers... », préc., *The Moscow Times*, 2022

l'Ukraine ; l'extrême droite ne conteste pas les raisons d'être de la guerre mais sa gestion fédérale ; et la section nationaliste est trop influente en Russie pour que l'État fédéral puisse se permettre de perdre son soutien – trois raisons qui expliquent probablement la tolérance de Vladimir Poutine à l'égard des blogueurs nationalistes russes diffusant les insuccès de l'armée russe⁷³⁸. La popularité des blogueurs nationalistes n'a cessé de croître jusqu'au début de 2023 au moins, faisant ainsi prospérer les images des échecs militaires et les critiques contre l'armée et le pouvoir politique sur les réseaux sociaux russes – à commencer par Telegram⁷³⁹. Depuis le début de la guerre, la critique contre le gouvernement fédéral n'a cessé de s'amplifier sur le réseau internet russe. Le Kremlin a ainsi perdu son principal soutien politique – l'extrême droite, dont la source de contestation autrefois incarnée par le seul opposant Alexeï Navalny s'est démultipliée en une diversité de foyers de contestation, chaque foyer influençant des centaines de milliers de russes.

B) Efficacité de la restriction russe à l'aune de la souveraineté numérique

1. La doctrine de la souveraineté numérique

Si la Fédération de Russie avait pour objectif de **privilégier les acteurs technologiques russes sur le marché russe en bloquant les acteurs étrangers**, la régulation d'internet opérée par la Russie est **très relativement efficace à court et moyen termes**. En effet, depuis 2014-2015, la Russie adopte la doctrine de la « souveraineté numérique » dans sa version nationaliste. La souveraineté numérique est une doctrine qui désigne l'application des principes de souveraineté aux technologies numériques, principalement aux réseaux numériques. Ces principes de souveraineté sont classiquement : la compétence des États (donc leur autorité) pour encadrer les technologies qui affectent leur population, leur territoire ou leurs administrations ; l'exclusivité de la compétence sur le territoire national et la plénitude des compétences internationales ; et l'indépendance des États et de leur population vis-à-vis des puissances technologiques privées et/ou étrangères.

Une première façon d'examiner la souveraineté numérique consiste à regarder le pouvoir exercé par les acteurs d'un réseau numérique comme une souveraineté comparable à celle de l'État. Dès 1996, le juriste Joel Reidenberg retrouve dans le réseau internet des éléments constitutifs de la souveraineté étatique : comme les citoyens adhèrent à une Constitution dans le cadre d'un contrat social, les internautes concluent des contrats d'adhésion avec les fournisseurs de services ; comme les citoyens tiennent leurs droits d'une Constitution, les internautes tiennent leurs droits des contrats passés avec les services ; comme l'État exerce ses pouvoirs de police sur le fondement de la Constitution, le service exerce ses pouvoirs de police sur le fondement du contrat d'adhésion⁷⁴⁰. Cette analogie entre services numériques et autorités

⁷³⁸ SAUER P., « "We have already lost"... », *The Guardian*, préc. 2022

⁷³⁹ DETTMER Jamie, « Pro-war Russia enraged over military failings », sur *Politico.eu*, 6 janv. 2023 ; « Russia now says 89 killed in Ukraine attack, blames mobile phones », sur *Aljazeera.com*, 4 janv. 2023

⁷⁴⁰ REIDENBERG Joel, « Governing Networks and Rule-Making in Cyberspace », *Emory Law Journal*, vol. 45, 1996, p. 912-930

gouvernementales, tous deux souverains, se poursuit encore aujourd'hui dans la littérature scientifique – à plus forte raison avec l'émergence de « géants d'internet »⁷⁴¹.

Une deuxième façon d'examiner la souveraineté numérique consiste à regarder les menaces que posent les technologies numériques pour la souveraineté de l'État. Cette deuxième lecture de la souveraineté numérique, fortement approfondie depuis les années 2000, a vu le jour à la même époque que la première. Ces deux éclairages de la souveraineté numérique ne sont pas toujours liés (on peut considérer que les technologies numériques menacent la souveraineté de l'État sans reconnaître aux acteurs de la technologie la qualité de souverains), mais sont tout à fait compatibles (on peut considérer que les technologies numériques menacent la souveraineté de l'État *parce que* les acteurs de la technologie sont souverains). Le premier éclairage (lecture paraétatique de la souveraineté numérique) étudie la manière dont les acteurs de la technologie appliqueraient une souveraineté paraétatique, tandis que le second éclairage (lecture étatique de la souveraineté numérique) étudie la manière dont l'État peut lui-même appliquer sa souveraineté aux technologies numériques.

La lecture étatique de la souveraineté numérique nous semble de loin la plus répandue dans les publications scientifiques actuelles⁷⁴². Elle a vu le jour à la même époque que la lecture paraétatique. On a déjà relevé que David Post et David Johnson estimaient le droit étatique inapplicable à internet en 1996⁷⁴³. En 2004, les philosophes marxistes Antonio Negri et Michael Hardt considèrent que les mouvements des biens, des personnes, des services et des informations opèrent désormais dans le cadre d'un réseau mondial de flux (économiques, numériques, migratoires...) assimilable à un Empire sans frontières. Ils en déduisent que les États peuvent de moins en moins réguler de tels mouvements à l'intérieur et autour de leurs frontières⁷⁴⁴. En Europe, les dangers du réseau pour la souveraineté étatique ont d'abord été théorisés à travers une opposition des concepts « réseau vs hiérarchie ». En 1980, les philosophes Gilles Deleuze et Félix Guattari observent la structure d'un rhizome (par ex. une racine de gingembre), et constatent que tout élément de cette structure peut influencer un autre sans

⁷⁴¹ BYK Christian, « L'ère du numérique conduit-elle à l'émergence de nouveaux acteurs et formes de souveraineté ? », *Cahiers Droit, Sciences & Technologies*, n° 15, 2022, p. 171-192 ; GU Hongfei, « Data, Big Tech, and the New Concept of Sovereignty », *Journal of Chinese Political Science*, mai 2023

⁷⁴² Leo Hippelainen, Ian Oliver et Shankar Lal définissent ainsi la « souveraineté des données » (*data sovereignty*) comme « le concept selon lequel l'information, qui a été convertie et stockée sous forme numérique binaire, est soumise aux lois du pays dans lequel elle se trouve » : HIPPELAINEN L., OLIVER I. et LAL S., « Towards dependably detecting geolocation of cloud servers » in YAN Zheng, MOLVA Refik, MAZURCZYK Wojciech et KANTOLA Raimo (dir.), *Network and System Security. 11th International Conference, NSS 2017, Helsinki, Finland, August 21-23 2017*, Springer, 2017, p. 643-656. D'autres auteurs ont plus récemment défini la souveraineté numérique comme « la capacité d'un État ou d'une fédération d'États à fournir les technologies qu'il juge essentielles à son bien-être, à sa compétitivité et à sa capacité d'action, et à les développer ou à les faire venir d'autres zones économiques sans dépendance structurelle unilatérale » : EDLER Jakob, BLIND Knut, FRIETSCH Rainer, KIMPELER Simone, KROLL Henning, LERCH Christian, REISS Thomas, ROTH Florian, SCHUBERT Torben, SCHULER Johanna et WALZ Rainer, « Technology sovereignty: from demand to concept », *Fraunhofer Institute for Systems and Innovation Research ISI*, 2020

⁷⁴³ JOHNSON D. et POST D., « Law and Borders – the Rise of Law in Cyberspace », *Stanford Law Review*, vol. 48, 1996, p. 1367s.

⁷⁴⁴ NEGRI Antonio et HARDT Michael, *Multitude: War and Democracy in the Age of Empire*, Penguin Books, 2004. Ces travaux sont repris en 2007 par la sociologue Allison Cavanagh, pour en conclure que le réseau internet a largement affaibli la souveraineté des États : CAVANAGH A., *Sociology in the Age of the Internet*, McGraw-Hill Education, 2007, p. 41-49.

être subordonné à élément (contrairement au modèle arborescent), sans dépendre d'une base (contrairement au modèle pyramidal), sans être concerné par un quelconque centre de la structure (contrairement au modèle centralisé)⁷⁴⁵. En 2000, s'inspirant notamment du rhizome de G. Deleuze et F. Guattari, les philosophes du droit François Ost et Michel Van de Kerchove estiment que le droit suit de moins en moins sa structure hiérarchique traditionnelle (droit imposé, élaboré dans un cadre national, produit et appliqué par les agents de l'État) au profit d'une structure en réseau (droit négocié, élaboré dans le cadre de relations internationales, produit et appliqué par des acteurs privés et publics)⁷⁴⁶.

Le réseau internet a souvent été tenu comme illustratif de la théorie de F. Ost et M. Van de Kerchove : la directive européenne « commerce électronique » de 2000 et sa transposition par la LCEN en France énoncent un « *programme d'actions* », des objectifs à atteindre (protection du consommateur et croissance du commerce électronique) davantage qu'un modèle fixe *a priori*, laissant ainsi aux acteurs privés une vaste marge pour leur action régulatrice⁷⁴⁷ ; les acteurs privés prennent des initiatives pour réguler les usages d'internet (interdiction des spams, politiques et chartes de conduite auxquelles adhèrent les utilisateurs, standards internationaux de protection de la vie privée...), définissent parfois les règles à l'issue d'un consensus avec les utilisateurs (comme Wikipédia), et contribuent de plus en plus à la production du droit par les États (les règles produites par les acteurs privées peuvent influencer celles produites par les États, peuvent se coordonner avec les règles étatiques...)⁷⁴⁸ ; le modèle juridique du droit d'auteur exclusif (tout type d'utilisation par un tiers d'une œuvre protégée est en principe interdit, sauf exceptions) est de plus en plus concurrencé par le modèle du logiciel libre (tout type d'utilisation par un tiers du logiciel libre est en principe autorisé, sauf exceptions)⁷⁴⁹. Le philosophe du droit Boris Barraud consacre une longue étude à la théorie de F. Ost et M. Van de Kerchove, pour vérifier sa validité dans le champ du réseau internet. Rapportant une inadaptation du modèle juridique pyramidal face à la production horizontale (« *hétérarchique* ») des règles de comportement sur internet, une inefficacité de la règle de droit qui découle de cette inadaptation, et une généralisation de l'élaboration et de l'application des règles par des acteurs privés, il interroge la souveraineté étatique : l'État est-il toujours souverain si la règle de droit est peu efficace sur internet, si se dissipe le monopole de l'État pour produire et exécuter des règles de conduite valant pour des millions voire milliards de personnes, si l'espace public dans lequel les populations discutent et agissent en ligne dépasse les frontières de l'État ?⁷⁵⁰

⁷⁴⁵ DELEUZE G. et GUATTARI F., *Mille plateaux. Capitalisme et schizophrénie*, Paris, Minuit, 1980, p. 32s.

⁷⁴⁶ OST François et VAN DE KERCHOVE Michel, « De la pyramide au réseau ? Vers un nouveau mode de production du droit ? », *Revue Interdisciplinaire d'études juridiques*, vol. 44, 2000, p. 1-82. Les philosophes belges ont approfondi leurs travaux dans l'ouvrage OST F. et VAN DE KERCHOVE M., *De la pyramide au réseau ?*, Bruxelles, F.U.S.L., 2002. Les auteurs y écrivent notamment (p. 14) : « avec le réseau, l'État cesse d'être le foyer unique de la souveraineté (...) ; les pouvoirs interagissent ; les juges deviennent des co-auteurs de la loi et les subdélégations du pouvoir normatif, en principe interdites, se multiplient ».

⁷⁴⁷ ROCHFELD Judith, « Les rapports entre la régulation et le contrat renouvelés par l'Internet », *Droit et économie de la régulation*, n° 4, 2006, p. 209-220

⁷⁴⁸ DUONG Lê-My, « Les sources du droit d'internet : du modèle pyramidal au modèle en réseau », *Recueil Dalloz*, 2010, p. 783s. : « une régulation privée se développe en marge du droit étatique »

⁷⁴⁹ VARNEROT Valérie, « La propriété littéraire et artistique en réseau », *Revue Communication – Commerce électronique*, mars 2013 ; v. aussi PELLEGRINI François et CANEVET Sébastien, *Droit des logiciels*, PUF, 2013, p. 141

⁷⁵⁰ BARRAUD B., *Repenser la pyramide des normes à l'ère des réseaux: Pour une conception pragmatique du droit*, préc., L'Harmattan, 2012

Toujours en Europe, le concept de « souveraineté numérique » apparaît timidement dans les années 2000. En avril 2004, Paris accueille un colloque paneuropéen appelant à développer une « *souveraineté technologique européenne* », en présence du Premier ministre et de plusieurs autres membres de gouvernement⁷⁵¹. Un nouveau colloque, tenu en novembre 2006 par la même organisation à Toulouse cette fois sur la politique spatiale et la souveraineté européennes, réitère son souhait de voir une « *souveraineté technologique* » européenne pour que l'UE soit en position de concurrencer économiquement l'Asie et les États-Unis dans le secteur⁷⁵². La même année, Bernard Benhamou et Laurent Sorbier évoquent une « *souveraineté numérique* » et semblent la définir comme la capacité de chaque État à réguler internet d'après un projet démocratique de façon qu'un seul État ou groupes d'États ne puisse contrôler à lui seul cette ressource technique⁷⁵³. En juin 2009, lors d'un colloque intitulé « souveraineté numérique », la ministre française de l'Intérieur déclare vouloir « *garantir la souveraineté numérique* », c'est-à-dire « *étendre à l'espace numérique le champ de l'État de droit* »⁷⁵⁴. Il faudra attendre 2011 pour que Pierre Bellanger, président de Skyrock, popularise le concept de souveraineté numérique à échelle européenne avec la définition suivante : « *la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux numériques* »⁷⁵⁵.

Les années 2013-2015 marquent un tournant pour la souveraineté numérique. En 2013, le Département américain de la justice (DoJ) enjoint Microsoft de lui laisser l'accès aux données personnelles de plusieurs utilisateurs de la messagerie Hotmail, contre lesquels un mandat de perquisition avait été émis dans le cadre d'une affaire de stupéfiants. Microsoft refuse de communiquer ces données aux autorités américaines, au motif que lesdites données sont hébergées sur les serveurs de Microsoft en Irlande – soit hors de la juridiction des États-Unis. En 2014, le juge de premier ressort donne raison au gouvernement : les entreprises américaines « *doivent remettre des informations privées lorsqu'elles reçoivent un mandat de perquisition valide des organismes américains d'exécution de la loi* ». En 2016, la Cour d'appel juge au contraire que « *les mandats de perquisition américains n'atteignent pas les données des clients [américains] stockées à l'étranger* ». L'affaire est portée par le DoJ devant la Cour Suprême, qui s'empare du dossier mi-octobre 2017. Les soutiens (notamment européens) à Microsoft se multiplient auprès de la Cour Suprême⁷⁵⁶, mais le législateur américain ne laissera pas à la Cour

⁷⁵¹ DARNIS Jean-Pierre, « La souveraineté technologique européenne, une réponse à la crise de la Covid-19 ? » [en ligne], *Fondation pour la Recherche Stratégique*, n° 41, mai 2020

⁷⁵² *Ibid.*

⁷⁵³ BENHAMOU Bernard et SORBIER Laurent, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006, p. 519-530 : « les autorités américaines, si elles reconnaissent que les ressources d'internet constituent pour les États un enjeu majeur de souveraineté, ont aussi réaffirmé, avant la seconde phase du sommet, qu'elles en garderaient le contrôle ultime. (...) Parce que ces technologies rendent l'information plus accessible, elles doivent aussi être sous-tendues par un projet démocratique : c'est la seule question qui vaille au regard de l'enjeu de la souveraineté numérique »

⁷⁵⁴ Colloque « souveraineté numérique » du 17 juin 2009, Intervention de Michèle Alliot-Marie, sur *interieur.gouv.fr*. La ministre de l'Intérieur juge indissociable la souveraineté numérique et la lutte contre la « *cybercriminalité* », entendue au sens large comme les infractions commises en ligne.

⁷⁵⁵ BELLANGER Pierre, « De la souveraineté en général et de la souveraineté numérique en particulier », *Les Échos*, 30 août 2011. La popularisation du concept s'intensifiera avec la publication de l'ouvrage BELLANGER Pierre, *La souveraineté numérique*, Stock, 2014

⁷⁵⁶ HERMANN Vincent, « Emails stockés en Irlande : Microsoft largement soutenue devant la Cour suprême américaine », *NextInPact*, 19 janv. 2018

l'occasion de résoudre le problème. En mars 2018, le Congrès adopte le CLOUD Act, qui légalise la possibilité pour l'administration américaine d'accéder aux des données hébergées à l'étranger si ladite administration se fonde sur un mandat ou l'autorisation d'un juge ⁷⁵⁷. Simultanément, le DoJ abandonne sa poursuite contre Microsoft, concédant qu'il n'y a « *plus de cas avéré (...) sur la question présentée* » en 2013⁷⁵⁸. La Cour Suprême prend acte de cet abandon en avril 2018, alors que le CLOUD Act avait un mois plus tôt tranché la question.

L'année 2013 est aussi celle des révélations par Edward Snowden de programmes de surveillance américano-britanniques ciblant les internautes du monde entier ont sensibilisé les États sur l'importance de sécuriser leurs infrastructures et leurs données contre des ingérences étrangères⁷⁵⁹. Dans un contexte de méfiance européenne à l'égard des traitements de données personnelles massives (« Big Data ») par les entreprises américaines (Google, Facebook, Microsoft, Apple, Amazon...), l'UE élargit le champ d'application territorial de son droit à la protection des données à caractères personnelles. Depuis 2014, elle l'étend ainsi à tout responsable de traitement qui dirige son activité vers le territoire européen et y possède un établissement, indépendamment du lieu où le traitement de données personnelles est effectué⁷⁶⁰. En 2015, les révélations de Snowden amènent la CJUE à juger que les niveaux de protection des données personnelles ne sont pas équivalents aux États-Unis et dans l'UE, et annule en conséquence le *Safe Harbor*⁷⁶¹. Parallèlement, se multiplient les investissements publics pour propulser les initiatives franco-allemandes : la boîte de messagerie en ligne De-Mail issue d'une loi allemande de 2008, le moteur de recherche Qwant lancé en 2013 et soutenu financièrement par la Banque européenne d'investissement en 2015, l'Initiative Européenne de Paiements née en 2020 et fondée par BNP Paribas pour les transactions en ligne, le projet de fourniture d'hébergement cloud Gaia-X en cours depuis 2019 et cofinancé depuis 2022 par la Banque centrale européenne....

En 2020, la pandémie de Covid19 fait prendre conscience à l'Union européenne qu'elle n'est pas autosuffisante technologiquement, en raison des problèmes d'approvisionnement en puces semi-conductrices (dont la production en Chine est mise à l'arrêt durant les confinements) et de la

⁷⁵⁷Clarifying Lawful Overseas Use of Data Act de mars 2018, Chapitre 4

⁷⁵⁸FILIPPONE Dominique, « Après le vote du Cloud Act, la Cour Suprême jette l'éponge face à Microsoft » [en ligne], *Le Monde Informatique*, 6 avr. 2018

⁷⁵⁹V. par ex. Sénat français, « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne », Rapport d'information n°696, 8 juil. 2014

⁷⁶⁰L'arrêt CJUE, *Google Spain*, 13 mai 2014, n° 131/12 a été le premier à étendre ainsi le champ d'application du droit de l'UE relatif à la protection des données personnelles, et l'art. 3 du RGPD de 2016 consacre cette évolution jurisprudentielle

⁷⁶¹CJUE, Gde ch., *Maximillian Schrems c/ Data Protection Commissioner*, C-362/14, 6 oct. 2015. Le *Safe Harbor* était un accord entré en vigueur en 1998, négocié entre l'UE et les États-Unis pour faciliter le transfert des données personnelles des citoyens européens vers les États-Unis. L'ancêtre du RGPD, la directive 95/46 sur la protection des données personnelles, conditionnait le transfert de données personnelles hors de l'UE par l'obtention d'une autorisation qui certifiait le respect par le responsable de traitement de la législation européenne. Cet accord certifiait par principe les responsables de traitement américains pour qu'ils puissent transférer les données hors de l'UE sans obtenir d'autorisation. Le *Safe Harbor* est renégocié entre la Commission européenne et le gouvernement des États-Unis sous le nom de *Privacy Shield* puis, le 8 juillet 2016, la plupart des États membres adhèrent au *Privacy Shield*. Ce dernier est à nouveau abrogé pour les mêmes motifs par la CJUE, *Data Protection Commissioner c/ Maximillian Schrems*, 16 juil. 2020, C-311/18.

dépendance du secteur de santé européen aux technologies étrangères⁷⁶². Souhaitant atteindre une indépendance technologique européenne, la Commission européenne propose en février 2022 un paquet législatif sur les semi-conducteurs pour « *garantir la sécurité d’approvisionnement, la résilience et la souveraineté technologique de l’UE* »⁷⁶³. En janvier 2023, la présidente de la Commission européenne Ursula Von der Layer érige explicitement la souveraineté numérique comme priorité de la Commission ⁷⁶⁴. Dans l’UE, le concept de souveraineté numérique a ainsi été propulsé depuis les années 2010 par les discours scientifiques alarmant de l’inefficacité territoriale et matérielle du droit étatique sur internet, par l’aggravation du retard technique de l’UE par rapport aux États-Unis et la Chine, par le traitement par des entreprises étrangères d’une quantité toujours plus volumineuse des données personnelles des citoyens européens, par les ingérences étrangères, et par la dépendance grandissante de l’UE à l’égard des technologies étrangères.

Troisièmement, outre les lectures étatique et paraétatique de la souveraineté numérique, on en relève une lecture individualiste. Selon cette lecture, le souverain numérique est l’utilisateur. Droit étatique et régulation privée sont ici tous deux appelés à mettre à disposition de l’utilisateur les informations, outils et mécanismes de protection pour lui permettre de contrôler souverainement les données qu’il produit ou qui l’identifient personnellement. Cette troisième lecture de la souveraineté numérique trouve ses prémices dans les années 1970. En 1977, l’Allemagne devient le premier pays à reconnaître à ses citoyens un droit à la protection de leurs données personnelles contre leur traitement par les organismes publics et les personnes physiques ou morales de droit privé⁷⁶⁵. La France la succède en 1978, avec la loi Informatique & Libertés dont la première phrase de l’article 1^{er} pose : « *l’informatique doit être au service de chaque citoyen* ». En 1983, au moment de juger la conformité à la Constitution d’une loi relative au recensement de la population, la Cour constitutionnelle allemande consacre le droit des citoyens à l’« *autodétermination informationnelle* », défini comme « *le droit de l’individu à déterminer par lui-même la divulgation et l’utilisation de ses données personnelles* »⁷⁶⁶. Aux États-Unis, la question du pouvoir de contrôle de l’utilisateur sur ses données était examinée sous un angle économique plutôt que sous celui de la vie privée. On a vu ainsi que, dès 1996, l’informaticien Keneth Laudon propose le versement d’un « *prix de compensation* » à l’utilisateur pour l’achat ou la vente de ses informations⁷⁶⁷. On a vu aussi que, dans les années 2000, les partisans de Yochai Benkler invitaient à renforcer les outils à disposition de tout utilisateur pour lui assurer de choisir les services et utilisateurs avec lesquels il communique⁷⁶⁸.

762 DARNIS J.-P., « La souveraineté technologique européenne, une réponse à la crise de la Covid-19 ? », préc., *Fondation pour la Recherche Stratégique*, 2020

763 « Souveraineté numérique : la Commission propose un paquet législatif sur les semi-conducteurs pour faire face aux pénuries et renforcer l’avance technologique de l’Europe », sur le site web de la représentation française de l’UE *France.representation.ec.europa.eu*, 8 fév. 2022

764 VELLIET Mathilde, « Souveraineté numérique : politiques européennes, dilemmes américains » [en ligne], *Institut français des relations internationales*, janv. 2023

765 Loi fédérale n° 7 S. 201 du 27 janv. 1977 portant protection contre l’emploi abusif de données à caractère personnel dans le cadre du traitement de données (Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung)

766 Cour constitutionnelle allemande, 15 déc. 1983, BVerfGE, tome 65, p. 1-71

767 LAUDON K. C., « Markets and privacy », *Communications of the ACM*, 1996

768 JOHNSON David, CRAWFORD Susan et PALFREY John, « The Accountable Internet », préc., *Virginia Journal of Law & Technology*, vol. 9, 2004, p. 7

Il faudra toutefois attendre la moitié des années 2010 pour que le contrôle de ses données par l'utilisateur soit rapporté à des enjeux de souveraineté. La surveillance généralisée des données par le gouvernement américain révélée par Edward Snowden en 2013 a laissé voir le manque de contrôle des utilisateurs sur leurs données. En 2016, l'UE intègre la préoccupation du contrôle de l'utilisateur sur ses données : tandis que cette préoccupation n'est nulle part mentionnée par la directive 95/46, le RGPD d'avril 2016 qui lui succède considère que « *les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant* »⁷⁶⁹. Dans cette perspective, le RGPD démultiplie les informations, droits et moyens de protection des citoyens européens à l'égard de leurs données personnelles. Est consacré leur droit au déréférencement (nouveau composant du droit à l'effacement) tel qu'issu de la jurisprudence *Google Spain*, leur droit à la portabilité de leurs données personnelles (droit pour l'utilisateur de récupérer auprès du responsable de traitement les données personnelles qu'il a produites, dans un format structuré, couramment utilisé et lisible par la machine, et droit pour l'utilisateur de transmettre ces données à un autre responsable de traitement), ou encore l'obligation pour le responsable de traitement d'informer ses utilisateurs en cas de violation de leurs données personnelles (i.e. en cas de « *violation de la sécurité entraînant (...) la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnelle (...) ou l'accès non autorisé à de telles données* »)⁷⁷⁰. Six mois plus tard, en s'inspirant du droit à l'autodétermination informationnelle consacré par la Cour de Karlsruhe, la loi française pour une République numérique retient une définition bien plus large du droit à la portabilité des données⁷⁷¹. En plus de réitérer le droit la portabilité des données personnelles prévu par le RGPD, cette loi confie au consommateur un droit générique à la portabilité de toutes ses données – personnelles ou non. Le consommateur peut ainsi récupérer, auprès du fournisseur de services de communication au public en ligne qu'il lui fournisse, toutes les données qu'il a produites, qui résultent de son compte utilisateur et/ou qui lui permettent de changer de service⁷⁷². La liberté est ensuite laissée à l'utilisateur de transférer les données récupérées vers un autre service en ligne. Depuis la fin des années 2010, de plus en plus de

769RGPD, cons. 7

770Ibid., respectivement art. 17 (droit à l'effacement), art. 20 (droit à la portabilité), art. 34 (information de la personne concernée par une violation de ses données à caractère personnel) et art. 4 (définition de la violation de données à caractère personnel)

771La secrétaire d'État chargée du Numérique et de l'Innovation qui a initié cette loi, Axelle Lemaire, déclarait ainsi : « *ce concept allemand jurisprudentiel de l'autodétermination informationnelle pourrait être traduit de façon plus simple en droit français. C'est une piste que nous souhaitons explorer* » (CUNY Delphine, « Données personnelles : le sujet polémique du futur projet de loi Numérique », *La Tribune*, 19 janv. 2015). Cette « traduction française » du droit à l'autodétermination informationnelle prendra la forme du droit à la portabilité des données dans la version finale du projet de loi (ZARKA Jean-Claude, « La loi pour une République numérique », sur *Actu-juridique.fr*, 26 oct. 2016)

772Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique, art. 48

chercheurs font référence à une souveraineté numérique de l'individu (parfois appelée « souveraineté des données »⁷⁷³) pour désigner le pouvoir de contrôle de l'utilisateur sur ses données⁷⁷⁴.

Tous les États ici étudiés (Union Européenne, Royaume-Uni, Russie, Chine, États-Unis) adoptent aujourd'hui la doctrine de la souveraineté numérique. La Chine et la Russie en font une interprétation nationaliste, *i.e.* une souveraineté numérique qui restreint l'accès des entreprises et organisations étrangères au marché technologique russe ou chinois. En Chine, la souveraineté numérique nationaliste a toujours accompagné le développement d'internet. La loi chinoise sépare les services de télécommunications en deux catégories : les services de télécommunication de base (BTS pour *Base Telecommunications Services*, 基础电信业务) qui « fournissent une infrastructure de réseau public, de transmission de données publiques et des services de communication vocale », ce qui inclut principalement les opérateurs téléphoniques, les FAI, les FAI, et les services VoIP comme WhatsApp, WeChat, Skype etc. ; et les services de télécommunications à valeur ajoutée (VATS pour *Value-Added Telecommunications Services*, 增值电信业务) qui « fournissent des services de télécommunication et d'information utilisant l'infrastructure du réseau public »⁷⁷⁵. Il est interdit aux investisseurs étrangers de détenir plus de 49% du capital d'un BTS (à l'exception des services de radiomessagerie qui peuvent être détenus à 100% par des investisseurs étrangers), de détenir plus de 50% du capital d'un VATS (à l'exception de certains services dont les investisseurs peuvent détenir 100% du capital⁷⁷⁶), et d'apporter le moindre apport en

⁷⁷³ En 2016, un groupe de chercheurs en informatique définit la souveraineté des données comme « le contrôle et la vérification de l'emplacement géographique des données » (ESPOSITO Christian, CASTIGLIONE Aniello et CHOO Kim-Kwang Raymond, « Encryption-Based Solution for Data Sovereignty in Federated Clouds », *IEEE Cloud Computing*, vol. 3, janv. 2016, p. 12-17). L'année suivante, deux autres informaticiens définissent la souveraineté des données comme « la capacité de l'utilisateur à posséder un contrôle total sur ses données » (ALBOAIE Sinica et COSOVAN Doina, « Private data system enabling self-sovereign storage managed by executable choreographies », *Lecture Notes in Computer Science LNCS*, juin 2017). L'expression *data sovereignty* est cependant ambiguë, parfois utilisée aussi pour désigner la souveraineté de l'État sur les données notamment dans le cadre de la politique de *cloud* souverain (HUMMEL Patrik, BRAUN Matthias, TRETTER Max and DABROCK Peter « Data sovereignty: A review », *Big Data & Society*, vol. 8, janvier-juin 2021)

⁷⁷⁴ GANASCIA Jean-Gabriel, GERMAIN Éric et KIRCHNER Claude, « La souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs », *Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene [CENA]*, oct. 2018 : « la notion de « souveraineté numérique individuelle » décrit la capacité des individus à maîtriser leurs données personnelles, médicales, pédagogiques (ex. scolaires, formation tout au long de la vie, etc.), mémorielles (photos, courriers, etc.) dans un contexte où la vision qu'ont les individus de la préservation de la vie privée dépend souvent de facteurs culturels et du niveau de maîtrise des outils numériques. (...) L'autonomie du sujet se heurte à la fois à la souveraineté nationale, comme cela a toujours été le cas dans les démocraties représentatives, et à la souveraineté entrepreneuriale, ce qui pourra engendrer des conflits dans le futur »

⁷⁷⁵ Conseil des affaires de l'État, Règlement de la République populaire de Chine sur les télécommunications (中华人民共和国电信条例) du 25 sept. 2005, art. 8 tel que modifié par les décisions du Conseil d'État 29 juillet 2014 et du 6 février 2016

⁷⁷⁶ Le capital d'un service de télécommunication peut être exclusivement apporté par des fonds étrangers pour les exceptions suivantes : les services de radiomessagerie, de transactions financières (commerce en ligne B2B, B2C, C2C etc.), de stockage et de transfert, les services d'accès Internet (hors VPN) situés dans la zone franche de Shanghai et sur l'île de Hainan qui ne fournissent pas d'infrastructure de réseau public ou de service VoIP comme les cybercafés, les services de diffusion de contenus (CDN, qu'on verra plus loin) situés sur l'île de Hainan, le service AppStore (magasin

capital aux services de centres de données (locaux accueillant des serveurs et/ou des équipements d'acheminement) situés en Chine. Pour exercer leur activité de télécommunication sur le territoire chinois, les services étrangers doivent donc le plus souvent établir une coentreprise sur le territoire chinois, à laquelle les investisseurs étrangers apportent au moins 25% du capital et au maximum 49% (pour les BTS) ou 50% (pour les VATS). La justice chinoise s'assure ainsi une compétence exclusive sur tout service de télécommunication qui exerce ses activités sur le territoire chinois, dès lors qu'un tel service doit être implanté sur le territoire chinois dans le cadre d'une coentreprise détenue majoritairement par des investisseurs chinois.

Par ailleurs, en 2022, la Chine restreignait – par blocage et/ou filtrage – l'accès à une cinquantaine au moins d'applications étrangères parmi les plus utilisées mondialement (presque tous les services d'Alphabet – société mère de Google – comme Google Search, Gmail, YouTube ou encore Blogspot, Facebook, Instagram, WhatsApp, Wikipedia, Archive.org, Reddit, Snapchat, Twitch, Steam Community, Messenger et Twitter sauf pour les touristes de Hainan, LinkedIn, Pornhub, Tumblr, Pinterest, SoundCloud, Dropbox, Medium, Dailymotion, BBC, The New York Times, Vimeo, The Guardian, Discord, Deviantart, DuckDuckGo, Viber, HBO...). En restreignant l'accès aux concurrents étrangers, la Chine privilégie l'essor des entreprises chinoises sur le marché chinois : WeChat n'a pas eu Facebook ni WhatsApp pour concurrents sur le marché chinois, Baidu Search n'a plus Google Search pour concurrent depuis 2010, tout comme Gaode Map et Baidu Map n'ont plus Google Map pour concurrent depuis 2010, Bilibili et Youku n'ont jamais eu YouTube pour concurrent, et NetEase Mail et QQ Mail n'ont pas Gmail pour concurrent, Baidu Knows n'a pas Quora pour concurrent, Kuaishou n'a plus Snapchat pour concurrent depuis la deuxième moitié des années 2010, Weibo n'a jamais eu Twitter pour concurrent sur le marché chinois, TikTok et Xiaohongshu n'a jamais eu Instagram pour concurrent sur le marché chinois, Meituan et Ele.me n'ont jamais eu Uber États pour concurrent, iQIYI et Tencent Video n'ont pas Netflix ni HBO pour concurrents (Netflix a lui-même bloqué son accès à la Chine), Kugou, QQ Music et Tencent Cloud Music n'ont pas Spotify ni SoundCloud pour concurrents (Spotify a lui-même bloqué son accès à la Chine) etc. Les blocages menés par la Chine sont certes assez aisément contournables mais, en faisant jouer la préférence nationale sur le réseau, ils ont largement bridé l'essor des concurrents étrangers au profit des entreprises chinoises. Combinés à l'interdiction pour les investisseurs étrangers d'apporter la majorité du capital des services de télécommunications agissant en Chine, ces blocages ont favorisé l'essor sur le marché chinois de géants indépendants des investisseurs étrangers (Tencent, Alibaba, Baidu, Xiaomi, ByteDance, Huawei, Sina, NetEase, Kingsoft...).

En Russie, la doctrine de la souveraineté numérique s'est d'abord exprimée à travers une loi de 2014 qui oblige les opérateurs de commerce électronique à stocker, sur des serveurs situés en Russie, une copie des données personnelles qu'ils collectent sur les Russes⁷⁷⁷. En 2015, la souveraineté numérique russe prend une tournure nationaliste. Cette année, la Chine et la Russie concluent un pacte de non-agression dans le cyberspace et de protection d'une « cyber-

d'applications d'Apple) dans la zone franche de Shanghai et sur l'île de Hainan, et les services de centres d'appels intérieurs et d'appels offshore. V. WANG Raymond, « China », *The Technology, Media and Telecommunications Review*, ed. 13, 6 janv. 2023 [en ligne sur *Thelawreviews.co.uk*]
⁷⁷⁷Loi n°242-FZ du 21 juil. 2014 portant modification de certains actes législatifs de la Fédération de Russie afin de clarifier la procédure de traitement des données à caractère personnel dans les réseaux d'information et de télécommunication (Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях")

souveraineté » selon les termes du pacte pour contrer la domination occidentale⁷⁷⁸. La même année, Vladimir Poutine annonce la préparation d'un projet de loi « pour un internet souverain », destiné à créer un réseau internet russe (« Runet ») capable de survivre en cas de déconnexion avec l'internet mondial⁷⁷⁹.

2. Évaluation de l'efficacité des restrictions en Russie pour le développement de sa souveraineté numérique

Dans ce contexte, on pense probable que le Kremlin ait voulu se saisir de l'opportunité de la guerre en Ukraine pour fermer le marché russe sur des réseaux sociaux russes, à l'image de la Chine. En effet, le blocage d'importants réseaux sociaux étrangers depuis la guerre en Ukraine (Facebook, Instagram, Twitter, TikTok) a profité à divers réseaux sociaux russes. D'après le fabricant russe Yota, l'un des principaux fabricants d'infrastructures haut débit mobile en Russie, le trafic à destination des réseaux sociaux russes a presque doublé entre janvier et novembre 2022 : la messagerie instantanée russe TenChat compte 95 fois plus d'utilisateurs en novembre qu'en janvier 2022, le réseau social de partage de contenus YARUS (partage d'images, vidéos et agrégateur d'actualités commentées) en comptait 2,7 fois plus, le réseau social russe de partage de courtes vidéos Yappy en comptait 2,5 fois plus, et la plateforme de partage de vidéos Rutube a elle aussi démultiplié le nombre de ses utilisateurs⁷⁸⁰.

Ainsi, d'après l'enquête de Yota, le nombre d'utilisateurs uniques mensuels de TenChat est passé de 1 500 à 150 000 entre janvier et novembre 2022, celui de Yappy est passé de 100 000 à 250 000 et celui de Rutube est passé de 5-6 millions à 10-11 millions. D'après la même enquête de Yota et sur la même période, le réseau social russe Odnoklassniki (OK, « Camarades de classe ») a vu le nombre de ses utilisateurs mensuels croître timidement de 37 millions à 40-41 millions en Russie (malgré une légère baisse d'utilisateurs au deuxième trimestre 2022)⁷⁸¹. Le nombre d'utilisateurs mensuels du réseau social VKontakte semble lui aussi avoir progressivement augmenté, passant de 73-75 millions (janvier 2022) à 76-78 millions (mars 2022) puis à 77-79 millions (mars 2023)⁷⁸².

778WEI Yuxi, « China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty »[en ligne], *The Henry M. Jackson School of International Studies*, 21 juin 2016

779On approfondira plus loin cette loi entrée en vigueur en 2019

780« Le trafic vers les réseaux sociaux et les messageries russes a presque doublé depuis le début de l'année : enquête de Yota » (Трафик на российские соцсети и мессенджеры увеличился почти в два раза с начала года: исследование Yota), sur *Cnews.ru*, 27 déc. 2022

781Ces résultats sont confirmés par l'enquête de Mediascope menée en février 2023 : ACHKASOVA Ksenia, « La consommation de médias en 2022 » (МЕДИАПОТРЕБЛЕНИЕ В 2022 ГОДУ), sur *Mediascope.net*, mars 2023 ; ils sont également confirmés par une légère augmentation du trafic vers Ok.ru recensée par la base de données SimilarWeb Pro sur les deux derniers trimestres 2022 ; pour les résultats d'OK au deuxième trimestre 2022, v. « L'audience mensuelle moyenne d'Odnoklassniki a diminué de 1,1 million de personnes au deuxième trimestre » (Средняя месячная аудитория "Одноклассников" во II квартале снизилась на 1,1 млн человек), *TASS* [journal russe d'État], 11 août 2022

782Statista rapporte que le nombre d'utilisateurs actifs de VKontakte a augmenté de 9% entre le dernier trimestre 2021 et le dernier trimestre 2022, v. MELKADZE A., « Number of average monthly active users of VK in Russia from 4th quarter 2021 to 4th quarter 2022 », sur *Statista.com*, 24 mars 2023. Mediascope rapporte que VKontakte a gagné près de 5 millions d'utilisateurs entre janvier et juillet 2022, v. KEFFER Laura, « Mediascope : l'audience d'Instagram a baissé de 5 fois en un an,

Plus que VK, OK ou Rutube, les internautes russes se sont surtout dirigés vers la messagerie instantanée Telegram après le blocage d'Instagram, Facebook, TikTok et Twitter. Le nombre d'utilisateurs mensuels de Telegram en Russie est ainsi passé de 31-33 millions en janvier 2022 à 44-46 millions en mars 2022, puis à 49-52 millions en mars 2023 (soit une hausse de la base d'utilisateurs mensuels de Telegram en Russie de 54-55% entre janvier 2022 et mars 2023, contre une hausse de 6-7% pour OK et pour VK)⁷⁸³. Surtout, Telegram est le réseau social sur lequel l'activité des utilisateurs s'est le plus densifiée depuis janvier 2022. D'abord, d'après le Centre Levada, les canaux Telegram (espaces de diffusion d'informations publiques par les utilisateurs qui rejoignent tel ou tel canal) ont vu leur audience tripler en Russie entre janvier et octobre 2022⁷⁸⁴. Cela signifie que, sur cette période en Russie, les interactions des utilisateurs de Telegram se sont nettement plus multipliées encore que le nombre d'utilisateurs de Telegram (lui-même multiplié par 1,55 entre janvier 2022 et mars 2023). Ensuite, d'après les quatre principaux opérateurs russes VimpelCom, MegaFon, Tele2 et MTS, le trafic internet (nombre de requêtes d'accès) à destination de Telegram s'est extraordinairement intensifié, surpassant en janvier 2023 le trafic russe à destination de WhatsApp, la messagerie instantanée la plus utilisée en Russie par son nombre d'utilisateurs⁷⁸⁵. Cela signifie que, en Russie, les utilisateurs de Telegram accèdent à Telegram bien plus souvent que les utilisateurs de WhatsApp accèdent à WhatsApp, et surtout qu'ils y partagent et y consultent bien plus d'informations. Enfin, d'après Mediascope, les utilisateurs de Telegram en Russie consacrent de plus en plus de temps à cette messagerie instantanée (38 minutes par jour en moyenne en mars 2023 contre 28 minutes en janvier 2022⁷⁸⁶). Parallèlement, l'audience de Facebook, Instagram, Twitter et TikTok a diminué entre janvier 2022 et avril 2023 (baisses respectives de

celle de Facebook de 3,5 fois » (Mediascope: аудитория Instagram за год упала в 5 раз, Facebook — в 3,5 раза), *Kommersant*, 4 mars 2023. On se méfie toutefois des évaluations de l'agence Mediascope, spécialisée depuis plus de 25 ans dans l'analyse du marché technologique russe, qui appartient pour plus de 80% au VTsIOM (Centre Panrusse d'étude de l'opinion publique) – un centre d'études et de sondages de plus en plus dépendant du Kremlin. On donne plus de crédit aux estimations du Centre Levada, une ONG composée principalement de chercheurs en sociologie, en psychologie et en marketing, fondée 2003 par le premier professeur russe de sociologie Iouri Levada après que ce dernier ait quitté le VTsIOM, le jugeant de plus en plus contrôlé et biaisé par le Kremlin. Le Centre Levada arrive à peu près aux mêmes résultats que ceux de Statista et de Mediascope dans ses enquêtes de mars et avril 2022, constatant à l'aide d'un sondage que 65% des répondants russes utilisent VKontakte (soit 90-95 millions avec une marge d'erreur de 5%, équivalant à un nombre mensuel d'utilisateurs de 80-81 millions sachant que, en moyenne, 8 à 12% des utilisateurs d'un réseau social en Russie s'y connectent une fois par mois, 74-76% s'y connectent quotidiennement et 10-14% s'y connectent une ou plusieurs fois par semaine) : v. « Internet, Réseaux sociaux et VPN » (Интернет, социальные сети и VPN), sur *Levada.ru*, 8 avril 2022

783« Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), sur *Levada.ru*, 18 avril 2023. Cette enquête d'opinions porte seulement sur les Russes âgés de plus de 18 ans, en précisant les tendances par tranches d'âge (en mars 2023, 78% des 18-25 ans utilisaient Telegram contre 17% des 55 ans et plus) ; en nous inspirant de ces tendances, on inclut dans notre évaluation les mineurs de 13-17 ans en Russie, en estimant que 65% à 85% d'entre eux (soit 2 à 3,5 millions) utilisent Telegram.

784« Les principales sources d'information des Russes » (Основные источники информации россиян), sur *Levada.ru*, 3 nov. 2022

785KEFFER Laura, « Telegram dépasse WhatsApp en termes de volume de trafic en Russie » (Telegram обогнал WhatsApp по объему трафика в России), *Kommersant*, 23 janv. 2023

786 IGNATIEV Dmitry, « L'audience d'Instagram a été divisée par 5 en un an de blocage, tandis que celle de Facebook a été divisée par 3,5 » (За год блокировки аудитория Instagram упала в 5 раз, а Facebook – в 3,5 раза), *Vedomosti*, 4 mars 2023

60%, de 45-50%, de 41%, et de 12%) ⁷⁸⁷ . Par conséquent, le blocage mené par la Russie a effectivement privilégié la croissance de réseaux sociaux russes (Telegram, VK, Odnoklassniki, Rutube) au détriment des réseaux sociaux étrangers bloqués (Facebook, Twitter, Instagram, TikTok).

A priori, les blocages ordonnés par la Fédération de Russie semblent donc avoir efficacement instauré une préférence nationale sur le marché numérique russe. Une telle conclusion doit néanmoins être nuancée par trois échecs importants. Premièrement, à l'exception de Telegram, **l'effet « préférence nationale » n'a profité aux services russes qu'à court terme** : en mars 2023, le nombre d'utilisateurs mensuels en Russie d'Odnoklassniki est retombé à 38-39 millions et celui de Rutube est redescendu à 5-6 millions⁷⁸⁸. Les deux réseaux sociaux ont donc retrouvé en avril 2023 leur audience mensuelle antérieure aux blocages de mars 2022. Quant à VK, il maintient une progression entre janvier 2022 et avril 2023 (+6-7% d'utilisateurs mensuels, de 73-75 millions à 77-79 millions) qui avait déjà débuté par une forte poussée entre mars 2021 et le dernier trimestre 2021 (+34-35% d'utilisateurs mensuels, de 52-54 millions à 72-73 millions)⁷⁸⁹. Sachant par ailleurs que VK est le deuxième réseau social le plus utilisé en Russie depuis 2018, on ignore si la progression de VK entre janvier 2022 et avril 2023 est due aux blocages de mars 2022 *ou bien* à la poussée de VK sur l'année 2021 (par effet de réseau, la hausse du nombre d'utilisateurs d'un réseau social augmente son utilité sociale et son attractivité) *ou encore* à une conjonction de ces deux facteurs (les blocages de mars 2022 ont favorisé l'effet de réseau de VK amorcé en 2021). Dès lors, à moyen terme, les blocages n'ont que peu profité aux réseaux sociaux russes – exception faite de Telegram.

Deuxièmement, **depuis les blocages, aucun géant internet russe n'a émergé, aucun nouveau service en ligne russe n'a suscité d'adhésion massive** de la part des utilisateurs. D'une part, la progression des nouveaux réseaux sociaux russes TenChat, Yappy et YARUS (respectivement 150 000, 250 000 et 1,7 millions d'utilisateurs mensuels en novembre 2022) est encore très loin de leur permettre de rivaliser avec les réseaux sociaux les plus utilisés en Russie. Le projet Rossggram, un réseau social censé se substituer à Instagram en Russie annoncé le 16 mars 2022, devait voir le jour le 28 mars 2022 mais, faute d'investissements et face aux difficultés de programmation, n'a cessé d'être reporté et n'est toujours pas ouvert au public en avril 2023 (disponible sur RuStore depuis le 9 février 2023 mais inutilisable)⁷⁹⁰. D'autre part, les grands réseaux sociaux russes de 2022 avaient déjà ce statut en 2021 : VK, OK et Telegram comptaient déjà parmi les réseaux sociaux les plus utilisés en Russie en janvier 2022, soit avant les blocages.

⁷⁸⁷ Pourcentages calculés à partir de l'étude du centre Levada d'avril 2023 : « Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), préc., sur *Levada.ru*, 2023

⁷⁸⁸ *Ibid.*

⁷⁸⁹ Cette poussée est notamment constatée par l'étude du Centre Levada de mars 2022, observant que la part de la population russe âgée de plus de 18 ans qui utilise VK est passée de 45% en mars 2021 à 65 en mars 2022 (« Internet, Réseaux sociaux et VPN » (Интернет, социальные сети и VPN), préc., avr. 2022) ; cependant, l'enquête précitée de Yota estime que le nombre d'utilisateurs unique de VK n'a pas augmenté entre janvier et novembre 2022. On en déduit que la poussée de VK rapportée par le Centre Levada s'est principalement produite entre mars et décembre-janvier 2021.

⁷⁹⁰ KASHEVSKY V., « La Russie a-t-elle réussi à créer un substitut... », préc., sur *Eurasianet.org*, 2022 ; TSEPELEVA Masha, « Le réseau social Rossggram prévoyait de lever 250 millions de roubles auprès d'investisseurs privés et promettait un rendement de 950 % sur trois ans » (Соцсеть «Россграм» запланировала привлечь 250 млн рублей от частных инвесторов и пообещала доходность 950% за три года), sur *Vc.ru*, 15 mars 2023

Lesdits blocages n'ont alors pas stimulé le marché russe au point de provoquer une percée des nouveaux et des anciens réseaux sociaux russes.

Troisièmement, **de nombreux réseaux sociaux occidentaux restent prééminents en Russie**. En effet, les réseaux sociaux russes ne sont pas les seuls à avoir progressé après les blocages. Sur la période mars 2022-mars 2023, l'audience de WhatsApp a bénéficié d'une croissance légèrement supérieure à celle de VK : 66% de la population russe âgée de plus de 18 ans utilisaient VK en mars 2023, contre 65% en mars 2022 (+1%) ; 70% de population russe âgée de plus de 18 ans utilisaient WhatsApp en mars 2023, contre 66% en mars 2022 (+4%)⁷⁹¹. Réseau social le plus utilisé en Russie depuis 2018 par le nombre de ses utilisateurs mensuels (84-87 millions)⁷⁹², WhatsApp a bénéficié sur le marché russe d'une croissance encore plus forte que VK, OK ou encore Rutube entre mars 2022 et mars 2023. Ironie du sort : l'application en ligne la plus utilisée en Russie est un produit de l'entreprise Meta, juridiquement qualifiée d'« organisation extrémiste » par les autorités russes depuis mars 2022 après que son PDG Mark Zuckerberg ait annoncé ne pas supprimer systématiquement les messages haineux (y compris les menaces de mort) contre les « envahisseurs russes »⁷⁹³.

Outre WhatsApp, YouTube reste de loin la plateforme de partage de vidéos la plus utilisée en Russie. On estime le nombre d'utilisateurs mensuels de YouTube en Russie entre 70-73 millions en mars 2023, en légère hausse (+4%) par rapport à mars 2022⁷⁹⁴. D'autant que les utilisateurs russes consomment nettement plus de contenus sur YouTube que sur Rutube – en décembre 2022, « le trafic de Rutube ne représent[ait] que 1 à 2% du trafic représenté par le segment russe de YouTube »⁷⁹⁵. Le moteur de recherche Google Search est le deuxième moteur de recherche le plus utilisé en Russie, où il rassemblait 58-62 millions d'utilisateurs mensuels en mars 2023 (contre 75-78 millions pour Yandex)⁷⁹⁶. L'audience de Facebook a certes perdu 55-60% de son audience mensuelle depuis janvier 2022 mais, même bloqué, il conserve 5-6 millions d'utilisateurs mensuels en mars 2023 soit autant que Rutube (pourtant promu). De même, Instagram a certes perdu 45-50% de son audience mensuelle depuis janvier 2022, mais on a vu qu'il conserve 25-27 millions (mars 2023) de ses 50-55 millions d'utilisateurs russes de janvier

⁷⁹¹ « Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), préc., sur *Levada.ru*, 2023

⁷⁹² *Ibid.* V. aussi les estimations proposée par Statista : « Average monthly number of users of Meta in Russia in January 2022, by platform » du 13 mai 2022, et « Number of daily active users (DAU) of WhatsApp and Telegram in Russia from September 1 to October 25, 2022 »

⁷⁹³ « Meta autorise certains messages anti-russes, Moscou riposte avec le blocage de Instagram », *La Tribune*, 11 mars 2022 ; « Russia confirms Meta's designation as extremist », *BBC*, 11 oct. 2022

⁷⁹⁴ « Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), préc., sur *Levada.ru*, avril 2023

⁷⁹⁵ KASHEVSKY V., « La Russie a-t-elle réussi à créer un substitut... », préc., sur *Eurasianet.org*, 2022

⁷⁹⁶ Estimations proposées à partir des études suivantes : « Most visited Yandex projects in July 2022, by monthly audience », *Statista*, mars 2023 ; les données proposées par StatCounter, une entreprise d'analyse Web dont le logiciel de suivi est installé sur plus de 1,5 millions de sites dans le monde (activités et emplacements géographiques), et qui s'appuie sur le nombre de pages consultées par les utilisateurs d'un service afin d'évaluer les parts de marché des différents services en ligne ; v. aussi « Comment les parts de Yandex et de Google en Russie et dans le monde ont évolué en 2022 ? » (Как в 2022 году изменились доли «Яндекса» и Google в России и мире), sur *Adindex.ru*, 22 fév. 2023 [Adindex est une société russe de publication en ligne spécialisée dans l'étude du marché de la publicité et du marketing en Russie]

2022. Le trafic russe à destination d'Instagram s'est néanmoins effondré, chutant de 81,7% entre janvier 2022 et janvier 2023, traduisant une diminution de l'activité des utilisateurs russes d'Instagram encore plus forte que la réduction de son audience en Russie (baisse de 45-50%). Le trafic perdu par Instagram semble toutefois avoir bénéficié à un autre réseau social occidental : Pinterest, dont le trafic russe a augmenté de 85,5% sur la même période au point d'égaler le trafic russe de VK⁷⁹⁷. L'essor de Pinterest depuis mars 2022 est complètement passé sous silence par les enquêtes officielles russes, et on peine à trouver des indices pour évaluer le nombre d'utilisateurs russes de Pinterest en mars 2023. En s'appuyant sur la hausse du trafic russe à destination de Pinterest recensée par StatCounter et par SimilarWeb entre janvier 2022 et janvier 2023, et sur une enquête de Kepios de novembre 2022, on estime le nombre d'utilisateurs mensuels de Pinterest en Russie entre 15 et 25 millions en mars 2023⁷⁹⁸.

En somme, **en mars 2023, le marché russe des réseaux sociaux et des moteurs de recherche n'a pas changé significativement par rapport à janvier 2022** et reste très partagé entre services russes et services occidentaux⁷⁹⁹. Les blocages ne nous semblent pas avoir privilégié la croissance des réseaux sociaux russes sur celle des réseaux sociaux occidentaux en Russie : entre mars 2022 et mars 2023, le trafic de Telegram a dépassé celui de WhatsApp et l'audience mensuelle de VK s'est légèrement étendue et l'activité des utilisateurs d'Instagram en Russie s'est effondrée ; mais l'audience de WhatsApp et le temps qu'y consacrent ses utilisateurs ont augmenté plus que ceux de VK, YouTube a progressé tandis que Rutube a chuté, et Pinterest a hérité du trafic d'Instagram pour égaler celui de VK. Les croissances et décadences des réseaux sociaux occidentaux sur le marché russe équivalent à peu près à celles des réseaux sociaux russes.

À plus long terme, on pense que les blocages de mars 2022 pourraient continuer à faire reculer l'audience d'Instagram en Russie, voire que Telegram pourrait dépasser l'audience mensuelle de WhatsApp sur le sol russe. Cependant, même à long terme, **on doute quelesdits blocages puissent à eux seuls bouleverser la pénétration des réseaux sociaux occidentaux sur le marché russe**. D'une part, les services en ligne occidentaux – réseaux sociaux (WhatsApp, YouTube, Pinterest...), moteurs de recherche (Google, Safari), navigateurs (Chrome), encyclopédie en ligne (Wikipedia, 35-45 millions d'utilisateurs mensuels en Russie⁸⁰⁰)... – sont fortement implantés sur

⁷⁹⁷ « Social Media Stats Russian Federation », sur *Statcounter.com*

⁷⁹⁸ *Ibid.* Pour l'enquête de Kepios, v. « Leading social media platforms in Russia in 3rd quarter 2022, by monthly penetration rate », *Statista*, 24 mars 2023

⁷⁹⁹ On propose le classement suivant des principaux réseaux sociaux, navigateurs et moteurs de recherche, de la plus grande à la plus petite audience mensuelle sur le sol russe en mars 2023 : 1. WhatsApp (84-87 millions d'utilisateurs actifs mensuels en Russie) ; 2. VK (77-79 millions) ; 3. Le moteur de recherche Yandex (75-78 millions) ; 4. Le navigateur Chrome (73-76 millions) ; 5. YouTube (70-73 millions) ; 6. Google Search (58-62 millions) ; 7. Telegram (49-52 millions) ; 8. Odnoklassniki (38-39 millions) ; 9. TikTok (37-39 millions) ; 10. Viber (29-31 millions) ; 11. Instagram (25-27 millions) ; 12. Le navigateur Yandex Browser (20-24 millions) ; 13. Pinterest (15-25 millions) ; 14. Zen (13-14 millions) ; 15. Discord (10-15 millions)

⁸⁰⁰ En 2015, Mediascope avait décompté 26 millions d'utilisateurs mensuels de Wikipedia en Russie (« TNS présente les premières données d'audience mobile pour les villes de plus de 700 habitants » (TNS представила первые данные по мобильной аудитории в городах 700+), sur *Mediascope.net*, 25 février 2015). En juillet 2019, Mediascope en dénombrait 29,4 millions pour 2,9 millions d'utilisateurs quotidiens dans les villes de plus de 100 000 habitants (MERZLIKIN Pavel, « Un analogue de Wikipédia va être créé en Russie. L'éditeur de l'Encyclopédie orthodoxe se chargera du

le marché russe. Cette implantation reflète l'attachement de dizaine de millions de russes à certains services occidentaux, et rend donc difficile l'évincement de ces services du marché russe. D'autre part, les blocages de certains réseaux sociaux occidentaux (Instagram, Facebook, Twitter) n'ont pas nui à la croissance d'autres réseaux sociaux occidentaux sur le marché russe (WhatsApp, YouTube, Pinterest). Les réseaux occidentaux peuvent continuer à s'implanter sur le marché russe tant qu'ils peuvent récupérer l'audience de ceux bloqués. Enfin, de nouveaux services occidentaux populaires pénétreront probablement le marché russe à l'avenir si rien ne les en empêche. Les restrictions de mars 2022 ne nous semblent donc avoir été que très relativement efficaces pour faire croître les réseaux sociaux russes et pour affaiblir la pénétration occidentale sur le marché russe. De ces blocages, **la Russie n'en ressort pas notablement plus indépendante vis-à-vis des entreprises occidentales.**

Section 2. La technique du filtrage

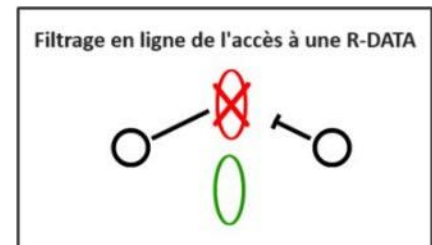
En adoptant toujours les mêmes critères de distinction que ceux utilisés jusqu'à présent, on différencie le filtrage pratiqué au niveau de la transmission de données (Paragraphe 1) et celui pratiqué au niveau du stockage de données (Paragraphe 2).

Paragraphe 1 – Le filtrage de la transmission de données

Le filtrage dès l'acheminement peut être pratiqué en ligne, auquel cas il est mis en oeuvre par une machine destinataire tierce (A), ou bien localement, auquel cas il est mis en oeuvre par la machine du producteur de données (B).

A) Le filtrage en ligne dès l'acheminement

On appelle « filtrage de l'accès à une R-DATA » la technique par laquelle le nœud destinataire empêche le nœud émetteur de produire une requête porteuse d'une R-DATA. Lorsque le filtrage est effectué dès l'acheminement, le routeur occupe la position du nœud destinataire par rapport au nœud émetteur (terminal ou serveur).



Le filtrage correspond à une configuration inverse à celle du blocage : la R-DATA *bloquée* est stockée par le nœud destinataire, mais le nœud émetteur est empêché d'y accéder ; la R-DATA *filtrée* n'est pas stockée par le nœud destinataire, mais produite ou stockée par le nœud émetteur. Au stade de l'acheminement, cette différence se traduit concrètement par le fait que le blocage agit sur toute information relative au destinataire bloqué (adresses IP, nom de domaine, URL...), tandis que le filtrage agit sur toute autre information contenue dans la requête d'accès émise (adresse de l'émetteur, contenu d'un message, code source porté par la requête, protocoles de communication requis...).

projet pour un montant de deux milliards de roubles » (В России создадут аналог «Википедии». Проектом за два миллиарда рублей займется издатель Православной энциклопедии), *Meduza*, 22 nov. 2019). En nous appuyant sur l'évolution du trafic organique (*i.e.* du trafic provenant d'un moteur de recherche) à destination de Wikipedia.org depuis la Russie recensée par Semrush, on estime le nombre d'utilisateurs mensuels de Wikipédia entre 35-45 millions.

Dans la Chine des années 2000, les opérateurs filtraient les contenus émis à l'appui d'une liste de mots-clés à filtrer⁸⁰¹. Depuis 2012, le gouvernement livre aux FAI des technologies de *deep packet inspection* (DPI), qui permettent d'analyser le trafic en temps réel et d'en déduire les données à censurer au niveau de l'acheminement⁸⁰². Activement mise en œuvre, la DPI a rendu possible le filtrage du darknet Tor, par reconnaissance de son protocole réseau particulier mentionné dans les requêtes qui y accèdent⁸⁰³. Elle est encore déployée pour filtrer l'accès à des VPN, bannis sur la base de leur protocole réseau par les opérateurs chinois⁸⁰⁴.

En Russie, c'est la loi sur l'internet souverain de 2019 qui oblige les opérateurs à installer des technologies de DPI « *pour contrer les menaces à la stabilité, à la sécurité et à l'intégrité du fonctionnement du réseau* »⁸⁰⁵. La même disposition précise par ailleurs qu'un opérateur « *n'est pas tenu de restreindre l'accès aux informations diffusées via le réseau d'information et de télécommunication « Internet », dont l'accès doit être limité conformément à la loi fédérale du 27 juillet 2006 sur l'information, les technologies de l'information et la protection de l'information* ». Cela signifie que les opérateurs ne sont théoriquement pas tenus de filtrer les contenus, programmes, services et sites illicites s'ils restreignent autrement et efficacement l'accès à ces informations illicites. À l'instar du dispositif chinois, la DPI russe pratique un filtrage par ralentissement – en ralentissant l'accès au destinataire au point d'entraîner l'expiration de la requête pour filtrer l'accès à des services tels que le réseau social Twitter ou le darknet TOR⁸⁰⁶.

En France, l'installation d'une technologie DPI est légalement autorisée pour les opérateurs depuis 2019. Néanmoins, la loi ne permet pas aux opérateurs d'employer cette technologie pour bloquer ou filtrer le trafic en temps réel, mais seulement pour analyser les paquets IP et « *détecter des événements susceptibles d'affecter la sécurité des systèmes d'information* » au moyen de « *marqueurs techniques* »⁸⁰⁷. La même disposition leur permet de conserver durant six mois les « *données techniques strictement nécessaires à la caractérisation* » d'un tel événement, dans le but dans permettre l'exploitation par l'Autorité nationale pour la sécurité des systèmes d'information (Anssi) qui coordonne nationalement la protection de la

⁸⁰¹ CLAYTON Richard, MURDOCH Steven et WATSON Robert, « Ignoring the Great Firewall of China », *Privacy Enhancing Technologies*, 2006, p. 20-35

⁸⁰² YANG Feng, The tale of deep packet inspection in China: Mind the gap, *3rd International Conference on Information and Communication Technology*, 2015

⁸⁰³ WINTER P. et LINDSKOG S., « How the Great Firewall of China is Blocking Tor », préc., *USENIX -FOCI'12*, 2012. Comme on l'a relevé plus haut, ces chercheurs de l'Université de Karlstad démontrent, après expérimentation du filtrage chinois, que le dispositif de DPI ralentit l'accès à l'IP destinataire, au point d'en empêcher l'accès.

⁸⁰⁴ TANG Chao, « In-depth analysis of the Great Firewall of China » [en ligne], *COMPT 116*, 2016

⁸⁰⁵ Loi fédérale n° 90 FZ modifiant la loi fédérale relative aux communications et la loi fédérale relative à l'information, aux technologies de l'information et à la protection de l'information du 1^{er} mai 2019, Art. 1^{er}, 3) c) ajoutant un §5.1 à l'art. 46 de la loi de 2003 relative aux communications

⁸⁰⁶ VITALIY Lapshichyov, « Technology of Deep Packet Inspection for recognition and blocking traffic of the Tor network » [en ligne], *XII International Conference on Security of Information and Networks*, Sochi 2019 ; NAST Condé, « Russia's Internet Censorship Machine Is Going After Tor » [en ligne], *Wired UK*, 2021

⁸⁰⁷ Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, art. 34 ajoutant un art. L 33-14 au du Code des postes et des communications électroniques (CPCE)

cybersécurité⁸⁰⁸. La DPI a ici pour objet d'identifier des logiciels malveillants et permettre à l'Anssi d'évaluer les moyens appropriés dans la lutte contre les cyberattaques⁸⁰⁹. L'Anssi peut elle-même imposer la mise en œuvre d'une DPI par tel ou tel opérateur « *lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des opérateurs [d'importance vitale⁸¹⁰] et des opérateurs [offrant des services essentiels au fonctionnement de la société et de l'économie]* »⁸¹¹. Dans ce cas, l'Anssi doit respecter les principes protégés par l'Arcep sous le contrôle de cette dernière⁸¹².

Nous n'avons pas trouvé, dans l'ordre juridique français, d'obligation légale de filtrage dès l'acheminement, pas plus qu'au Royaume-Uni ni aux États-Unis, ni même dans l'UE. Cela ne signifie pas pour autant qu'un filtrage dès l'acheminement serait illégal ou inconventionnel. On distingue les mesures de DPI issues de la loi (DPI d'initiative légale) des mesures de DPI décidées par les opérateurs (DPI d'initiative privée).

Concernant la DPI d'initiative légale, lors de la préparation du règlement 2015/2120 pour un internet ouvert, le Conseil de l'UE était interrogé sur conformité du système britannique de restriction par défaut au principe de neutralité d'internet, alors que le Royaume-Uni était encore membre de l'UE. En 2015, le Conseil y a répondu que le principe de neutralité est compatible avec les obligations que « *les utilisateurs finals (...) devraient respecter (...) en vertu du droit de l'Union ou du droit national (...) si des mesures [leur] interdisent d'accéder à des contenus illicites* »⁸¹³. Cette position s'accorde avec celle de la Commission européenne, qui proposait

⁸⁰⁸ L'Anssi est une autorité administrative non indépendante du pouvoir exécutif, rattachée au Secrétariat National de la Défense et de la Sécurité Nationale (Premier Ministre)

⁸⁰⁹ Le législateur parlait d'ailleurs de « marqueurs d'attaques » : v. étude d'impact sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense du 6 fév. 2018, p. 128

⁸¹⁰ Le Code de la défense définit les opérateurs d'importance vitale comme « *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* » (art. L. 1332-1) ainsi que les « *établissements [toute personne physique ou morale, publique ou privée]* » pour lesquels « *la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population [installations nucléaires de base et installations pouvant présenter des dangers ou inconvénients pour la commodité du voisinage, la santé, la sécurité et la salubrité publiques, l'agriculture, la protection de la nature, de l'environnement et des paysages, l'utilisation économe des sols, l'utilisation rationnelle de l'énergie, la conservation des sites et monuments et du patrimoine archéologique]* » (art. L1332-2 du Code de la défense et L511-1 du Code de l'environnement)

⁸¹¹ Loi de programmation militaire 2019-2025, art. 34 ajoutant un art. L2321-2-1 au Code de la défense.

⁸¹² *Ibid.*, art. 34 ajoutant un art. L2321-5 au Code de la défense. Pour la première fois, l'Anssi est soumise à une autorité administrative indépendante. Les principes protégés par l'Arcep sont : l'égalité et loyale concurrence non discriminée entre opérateurs au profit de l'accès des consommateurs au réseau ; la préservation de l'accès matériel des consommateurs au réseau de leur choix ; la garantie de l'accès matériel des personnes handicapées aux services et équipements ; le principe de neutralité du réseau ; le respect de la cybersécurité et de l'ordre public ; le respect du droit à la vie privée et la protection des données personnelles par les opérateurs ; la cohérence du réseau (couverture territoriale du réseau, interopérabilité des opérateurs, neutralité...) ; la protection des consommateurs contre l'exposition aux champs électromagnétiques etc. (art. L32-1 CPCE)

⁸¹³ Conseil de l'Union européenne, 2013/0309 (COD), 20 janvier 2015

dans son projet de règlement que les opérateurs puissent, par exception au principe de neutralité, prendre des mesures de gestion du trafic, pour « *bloquer, ralentir, dégrader ou traiter de manière discriminatoire des contenus, applications ou services* » si ces mesures sont « *nécessaires* » et qu'elles « *mettent en œuvre une disposition législative ou une décision de justice, ou prévenir ou lutter contre les infractions graves* »⁸¹⁴. La version définitivement adoptée autorise les opérateurs à recourir à des mesures de gestion du trafic « *pour se conformer aux actes législatifs de l'Union ou à la législation nationale qui est conforme au droit de l'Union* »⁸¹⁵. Constitutive d'une telle mesure de gestion du trafic, une DPI d'initiative légale est donc compatible avec la neutralité si elle est conforme au droit de l'UE – notamment à la Charte des droits fondamentaux de l'Union européenne. Dès lors, le cadre juridique européen semble concéder qu'une obligation légale de filtrage puisse être conforme au droit de l'UE. Ainsi, en France, bien que seule était concernée la DPI pour analyse et non pour filtrage, l'Arcep admet que le pouvoir de l'Anssi d'obliger les opérateurs à employer une technologie de DPI à des fins d'analyse est conforme au respect des correspondances privées et au principe de neutralité d'internet, pourvu que l'analyse s'en tienne aux métadonnées sans explorer le contenu des communications et que le recours à cette technologie n'empêche pas le bon fonctionnement du réseau⁸¹⁶.

Concernant la DPI d'initiative privée, au Royaume-Uni⁸¹⁷ comme aux États-Unis⁸¹⁸, de nombreux opérateurs ont décidé par eux-mêmes de déployer une DPI pour filtrer les partages de fichiers attentatoires au droit d'auteur. Aux États-Unis, on a vu que les opérateurs peuvent restreindre l'accès à toute information « *répréhensible* » sans voir leur responsabilité engagée de ce fait, ni se voir opposer une violation de la liberté d'expression. On a vu par ailleurs que le principe de neutralité n'est pas en vigueur sur le territoire américain, et ne peut donc s'opposer aux restrictions initiées par les opérateurs, y compris au moyen d'une DPI.

Au Royaume-Uni, le principe de neutralité d'internet est consacré depuis 2011 avec une certaine souplesse. Il résulte de lignes directrices émises par l'Ofcom, autorité britannique de régulation des communications dont les compétences couvrent celles de l'Arcep et de l'Arcom françaises. L'Ofcom définit la neutralité d'internet à partir de deux droits des consommateurs : celui d'obtenir les informations suffisantes pour leur permettre de prendre les bonnes décisions d'achat ; et celui de changer de FAI⁸¹⁹. Les lignes directrices autorisent les opérateurs à pratiquer une gestion du trafic tant qu'ils respectent ces deux droits, mais estiment qu'il y a « *une attente que tout opérateur fournisse sans restriction l'accès à tout service légalement*

⁸¹⁴ Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, et modifiant les directives 2002/20/CE, 2002/21/CE et 2002/22/CE ainsi que les règlements (CE) n° 1211/2009 et (UE) n° 531/2012, COM/2013/0627 final*, 11 sept. 2013, art. 23, 5 a)

⁸¹⁵ Règlement 2015/2120 (UE) pour un internet ouvert, art. 3 a)

⁸¹⁶ Arcep, Avis n° 2018-0101 du 30 janvier 2018 sur des dispositions relatives à la sécurité et à la défense des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2019-2025, p. 3-4

⁸¹⁷ JACKSON Mark, « Virgin Media UK Trial Deep Packet Inspection to Track Illegal File Sharing » [en ligne], sur *ISPReview UK*, 2009

⁸¹⁸ MUELLER Milton L. et ASGHARI Hadi, « Deep packet inspection and bandwidth management », *Telecommun. Policy*, 36, 2012., p. 462-475

⁸¹⁹ Ofcom, *Ofcom's approach to net neutrality*, 24 nov. 2011, point 1.7

disponibles [ou souligne] »⁸²⁰. L'Ofcom accepte également les restrictions effectuées « *à des fins commerciales* ». Chaque opérateur peut élaborer sa propre politique de restriction s'il « *fournit aux consommateurs la capacité de prendre des décisions suffisamment éclairées ou si est trop élevé le risque que les consommateurs soient trompés sur le service qu'ils paient* », en mettant à la disposition des consommateurs « *des informations claires et intelligibles sur la gestion du trafic, ses raisons et son impact, ainsi qu'un tableau commun comparant les politiques de gestion du trafic de chaque forfait, afin de permettre aux consommateurs de comparer les offres diverses* »⁸²¹. En juin 2016, un peu moins de trois semaines avant les résultats du référendum sur le Brexit, le think tank du gouvernement britannique « Broadband Stakeholders Group » publie le code de conduite *Open Internet Code*, qui définit la neutralité du réseau en s'inspirant de la définition posée par le règlement européen 2015/2120. D'après ce code, « *les mesures de gestion de trafic qui vont au-delà d'une gestion raisonnable du trafic peuvent seulement être appliquées dans les cas autorisés par le règlement de l'UE* »⁸²². Le code propose ensuite une liste non exhaustive de restrictions qu'il juge conforme au cadre juridique européen, telles que les restrictions aux fins de protéger la sécurité et l'intégrité du réseau (restriction des malwares, spam...), le blocage de sites et de services requis par la loi, l'usage de mécanismes de vérification de l'âge, de contrôle parental et de protection des mineurs, ou encore les restrictions par application du contrat (limitation des téléchargements, utilisation gratuite de certains services au détriment d'autres...). Ce code de conduite est aujourd'hui suivi par la plupart des opérateurs britanniques⁸²³. Le Royaume-Uni conserve donc sa définition de la neutralité d'internet comme une fourniture d'internet sans restriction d'accès aux contenus et services dont l'accès est légal ou dont la restriction n'est pas prévue dans le contrat de fourniture. Un filtrage par DPI d'initiative privée n'est donc pas contraire au principe de neutralité si elle cible des services ou contenus contraires à la loi ou au contrat.

Pour ce qui est de la France, en 2013, dans une réponse à la question d'une députée, la ministre de la Justice n'excluait pas que les opérateurs puissent légalement prendre l'initiative de pratiquer une DPI, s'ils respectent le secret des correspondances privées⁸²⁴. En 2019, des chercheurs et ONG suspectaient 186 opérateurs de recourir à une DPI, notamment dans le cadre des pratiques de *zero rating* (non-facturation à l'abonné, par l'opérateur, de l'accès à certains services au détriment d'autres) pour facturer différemment les paquets IP selon les services destinataires, ou encore ralentir l'accès à certains services en renvoyant les paquets vers des routeurs déjà surchargés⁸²⁵. Le règlement 2015/2120, dont l'application est d'effet direct dans le droit français contrairement au droit britannique, réduira peut-être le champ laissé aux restrictions initiées par les opérateurs européens y compris français. Ce texte n'autorise l'emploi de mesures de gestion du trafic d'initiative privée que si lesdites mesures sont destinées à « *préserver l'intégrité et la sûreté du réseau* » ou à « *prévenir une congestion imminente du réseau et*

⁸²⁰ *Ibid.*, point 1.10

⁸²¹ *Ibid.*, point 1.14

⁸²² Broadband Stakeholders Group, *Open Internet Code of Practice*, 8 juin 2016, Engagement n°3

⁸²³ JACKSON Mark, « Ofcom Begin New Review of UK Net Neutrality Rules Post Brexit UPDATE » [en ligne], sur *ISPreview UK*, 7 sept. 2021

⁸²⁴ « Question n°23790 - Assemblée nationale », [consulté le 21 août 2022].

⁸²⁵ European Digital Rights, « Open lettre to European policymakers and regulators warning against the widespread use of privacy-invasive Deep Packet Inspection technology in the EU » [en ligne], sur *European Digital Rights (EDRI)*, 15 mai 2019

atténuer les effets d'une congestion exceptionnelle et temporaire du réseau »⁸²⁶. En 2020, et à la différence de l'interprétation britannique de ce principe⁸²⁷, la CJUE juge la pratique commerciale de *zero rating* contraire au principe de neutralité d'internet⁸²⁸, mais n'est pas interrogée et ne se prononce pas sur la compatibilité des DPI d'initiative privée avec ce même principe de neutralité. On ignore donc si les opérateurs européens peuvent prendre l'initiative de filtrer ou de bloquer des contenus illicites, mais le droit de l'UE semble le leur interdire à des fins commerciales ou contre des services et contenus licites.

Le filtrage présente le même avantage que le ralentissement et le blocage, à savoir la possibilité de cibler des R-DATA spécifiques à un type de contenus, de services ou de programmes. Sur ce terrain, le filtrage est même la technique plus précise en ce qu'elle donne le pouvoir de cibler n'importe quelle information contenue dans un paquet IP – à l'exception des informations relatives au destinataire, qui relèvent de la technique de blocage. On a vu par ailleurs que le filtrage peut être associé au ralentissement si le routeur filtreur ralentit la requête au point d'en faire expirer la validité. Cette association a pour double intérêt de cibler la restriction avec une bonne précision tout en pénalisant la patience du prescripteur qui tente d'accéder à la R-DATA. Ainsi, on a vu que le système chinois de restriction des contenus, services et programmes constitutifs de R-DATA est un système (le « Grand Pare-feu de Chine ») qui combine blocage, filtrage et ralentissement. La précision du filtrage par rapport au blocage réduit fortement du risque de sur-filtrage par rapport au risque de sur-blocage.

Le filtrage en ligne a néanmoins deux inconvénients de taille. Tout d'abord, il est financièrement et techniquement assez lourd à supporter. Financièrement, les petits opérateurs n'ont généralement pas les moyens d'assumer le coût d'une technologie DPI, de sorte que le filtrage ne peut être efficace que : si les petits opérateurs dépendent fortement de grands opérateurs nationaux pour fournir un accès internet (*i.e.* si le réseau est centralisé), auquel cas le filtrage par les grands opérateurs suffit à couvrir tout le réseau national ; ou si l'État est en mesure de prendre en charge les frais des petits et moyens opérateurs. Techniquement, le filtrage requiert une analyse de chaque paquet, ce qui consomme beaucoup des ressources des routeurs, ralentit voire paralyse ou détourne leur trafic vers les mauvais destinataires lorsque survient un trafic anormal ou une incompatibilité entre le logiciel de filtrage et les programmes du routeur⁸²⁹. Ces inconvénients tant financiers que techniques se sont tous illustrés en Russie comme on le relèvera un peu plus loin, faute d'un réseau centralisé de l'acheminement et

826Règlement 2015/2120 pour un internet ouvert, art. 3 a)

827L'Ofcom admet la pratique de *zero rating* : Ofcom, *Ofcom's approach to assessing compliance with net neutrality rules. Frameworks for assessing zero rating offers and traffic management measures for compliance with the Open Internet Regulation*, 16 mai 2019

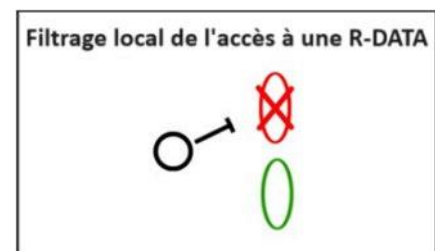
828CJUE, *Telenor Magyarország* préc., 15 sept. 2020, aff. C-807/18

829On l'observe en Russie : GAVRILYUK Anastasia, « Le blocage se renforce » (Блок крепчает), *Kommersant.ru*, mars 2022 : « Selon le spécialiste informatique indépendant Philip Kulin, tous les opérateurs russes n'ont pas installé le TSPU [ТСПУ nom donné à la technologie DPI employée] : "En outre, l'équipement peut ne pas être installé sur tous les réseaux et ne pas toujours fonctionner correctement." Oleg Blinov, enseignant à l'école numérique de Moscou, note que personne ne sait exactement comment fonctionne le TSPU. Dans les conditions économiques actuelles, les réserves d'équipements des opérateurs de télécommunications seront suffisantes pour assurer l'opérabilité de l'infrastructure pendant quatre à six mois, prédit la Commission des communications et des technologies de l'information du RSPP. Ainsi, le risque d'accidents et de perturbations de la stabilité du réseau augmentera de juillet à août »

d'investissements publics suffisants. Certes moins précis, le blocage est plus simple d'utilisation et moins coûteux mais, utilisé contre un grand nombre de sites ou de pages internet, le blocage implique une gestion coûteuse et peu pratique de bases de données (« listes noires ») très évolutives⁸³⁰ et volumineuses des services et contenus censurés. Lorsqu'un grand nombre de sites, de pages ou de contenus est en jeu, le filtrage est donc une très utile pour compléter les limites du blocage si les conditions techniques et financières le permettent. Le deuxième inconvénient de taille du filtrage en ligne est commun au ralentissement et au blocage : le filtrage en ligne est assez aisément contournable – on l'expérimentera. Face à la facilité de contournement, la lourdeur technique et financière du filtrage en ligne peut facilement aboutir à une régulation contre-productive lorsque le réseau n'est pas centralisé ou lorsque l'État manque de moyens financiers.

B) Le filtrage local dès l'acheminement

Le filtrage dès l'acheminement ne relève pas nécessairement d'une configuration « en ligne ». Il peut aussi survenir dans une configuration locale, qui implique une seule machine à la fois émettrice et destinataire des requêtes produites sur cette machine. La machine étant son propre destinataire, le filtrage se traduit localement en empêchant, depuis la machine d'un prescripteur, ce même prescripteur de produire ou stocker une R-DATA. Lorsque le filtrage local est effectué dès l'acheminement, le routeur occupe la position du nœud à la fois émetteur et destinataire, *i.e.* du nœud qui se voit empêché de faire stocker une R-DATA.



Un moyen couramment adopté par les États consiste à empêcher des personnes physiques ou morales d'obtenir la qualité d'opérateur pour les priver du pouvoir de fournir sur le territoire de cet État un réseau connecté à internet. Les opérateurs sont dans ce cas filtrés avant même de pouvoir fournir un accès internet, et donc avant même de permettre potentiellement le stockage de R-DATA. En Chine, on a vu que, pour exercer leur activité, tout opérateur de transmission doit préalablement obtenir une licence VATS, qui interdit les investisseurs étrangers de détenir plus de 50% du capital de cet opérateur. On a aussi souligné que ce plafonnement des capitaux étrangers assure à l'État chinois une compétence sur toutes les données transmises par les opérateurs exerçant leur activité sur son territoire, y compris les données refusées par le droit chinois (transmission de données anonymes, de rumeurs, de propos haineux, de divulgations de secrets d'État, de requêtes d'accès à des contenus pornographiques...).

Parmi ces opérateurs à capitaux nationaux, trois d'entre eux bénéficient d'importants investissements publics : China Telecom, China Mobile et China Unicom, dont l'État est actionnaire majoritaire⁸³¹. Ce soutien de l'État provoque une distorsion de concurrence sur le

⁸³⁰Les adresses IP, noms de domaine et/ou URL des services et contenus illicites changent régulièrement, sans compter sans compter l'actualisation des bases par l'ajout régulier de nouveaux sites et contenus bloqués

⁸³¹L'État détient 70.89% de China Telecom (rubrique « Directors, Supervisors and Senior Management » sur le site de China Telecom), 60% de China Unicom (profil de l'entreprise « China Unicom (Hong-Kong) Ltd. » sur le site web de Nikkei Asia), et 72.7% de China Mobile (profil de

marché des opérateurs téléphoniques en privilégiant ces trois opérateurs sur les opérateurs privés, ayant pour double effet : d'assurer aux trois opérateurs d'être, de loin, les trois principaux sur le marché⁸³² ; de garantir à l'État, actionnaire majoritaire, d'être la première source économique de pression au sein de ces trois entreprises oligopolistiques. En filtrant les candidats à la fourniture d'un service d'accès internet selon un critère de nationalité de la provenance de leurs capitaux, et en quasi-nationalisant les opérateurs de son choix, l'État préserve sa compétence exclusive sur le trafic chinois et s'accorde un puissant contrôle économique sur les trois opérateurs qui concentrent 99.9% des abonnés sur le marché.

En Russie, on a rapporté que les opérateurs doivent acquérir un certificat de média de masse pour exercer leur activité sur le territoire. Le candidat à la fourniture de service d'accès internet se voit octroyé ce certificat par le Roskomnadzor⁸³³. Le certificat se décline sous diverses licences : si la fourniture d'accès internet s'accompagne d'une offre d'abonnement, le candidat doit obtenir licence pour les services de communication télématique et la licence pour les services de transmission de données à l'exception des données vocales, auxquelles peut s'ajouter la licence pour la fourniture de canaux de communication si l'opérateur dispose d'équipements dans différents lieux physiques ; si la fourniture d'accès internet se fait par voie satellitaire, il doit obtenir au moins la licence pour les services de radiocommunication mobile par satellite ; si la fourniture d'accès internet se fait au moyen de réseaux téléphoniques, il doit obtenir la licence pour les services de communication télématique, la licence pour les services de transmission de données vocales, la licence pour la fourniture de services téléphoniques dans un réseau de communication locaux et/ou dédié etc.⁸³⁴ Par exemple, un cybercafé nécessite l'obtention des deux premières licences citées car il propose des offres d'abonnement pour accéder à internet⁸³⁵. Inversement, un bar, un restaurant ou un hôtel est

l'entreprise China Mobile sur Zonebourse.com). Ces groupes, principalement China Unicom, font l'objet depuis 2015 d'une réforme de la propriété mixte (*mixed-ownership reform*), qui consiste à diversifier les investisseurs se partageant les parts non-détenues par l'État en invitant les holdings de ces groupes à revendre l'unité d'action que possède chaque holding à des investisseurs privés pouvant chacun détenir 30 à 45% de cette unité (WANG Jiangyu, « The State As Controlling Shareholder in Chinese State-Owned Enterprises », *SSRN Electronic Journal*, 2018).

832En 2020, China Mobile représentait 52.54% des parts de marché, China Telecom 26.67% et China Unicom 20.78%, de sorte que les trois entreprises couvrent à elles seules 99.99% des parts de marché : v. « [L'industrie en profondeur] Aperçu 2022 : paysage concurrentiel et part de marché de l'industrie chinoise des communications (concentration du marché, évaluation de la compétitivité des entreprises etc.) » (« 【行业深度】 洞察 2022 : 中国通信产业竞争格局及市场份额(附市场集中度、企业竞争力评价等) », sur *Finance.sina.com*, 15 mars 2022 [consulté le 26 août 2022]

833Loi fédérale n° 126 FZ relative aux communications (Федеральный закон о связи), 7 juil. 2003, art. 29

834Décret fédéral n° 2385 du 30 déc. 2020 relatif aux activités d'octroi de licences dans le domaine des services de communication et à l'invalidation de certains actes du gouvernement de la Fédération de Russie (Постановление Правительства РФ "О лицензировании деятельности в области оказания услуг связи и признании утратившими силу некоторых актов Правительства Российской Федерации")

835Les personnes qui fournissent des services de communication à des abonnés « pour la réception et la transmission de messages électroniques télématiques » sont soumises à l'obligation d'obtenir une licence télématique (*ibid.*, art. XVI). Or, la loi russe définit un « message électronique télématique » comme « un ou plusieurs messages de télécommunication contenant des informations structurées conformément à un protocole d'échange pris en charge par le système d'information et le terminal d'abonné coopérants » (décret fédéral n° 575 relatif à l'approbation des règles de fourniture de

exempté de toute licence auprès du Roskomnadzor s'il fournit à ses clients et salariés un accès internet sans proposer d'offre d'abonnement à cette fin, mais doit préalablement s'enregistrer auprès du Roskomnadzor⁸³⁶. Le Roskomnadzor peut refuser de délivrer une licence s'il estime que « l'activité déclarée par le demandeur de la licence n'est pas conforme aux exigences et règles établies pour ladite activité »⁸³⁷. Or, la loi oblige les opérateurs à mettre en œuvre le blocage et le filtrage des services et contenus inscrits dans le registre du Roskomnadzor. Ce faisant, les licences incluent l'obligation pour les opérateurs de bloquer et filtrer les contenus conformément à l'art. 15.1 de la loi relative à l'information de 2006, même lorsque la fourniture d'accès internet se fait par Wi-Fi à destination d'un public (cybercafés, lieux accessibles aux enfants, établissements d'enseignements...)⁸³⁸. Sur le marché russe, les candidats à la fourniture d'un service d'accès internet sont donc filtrés à partir, entre autres, de leur engagement à restreindre l'accès aux contenus illicites.

Le marché russe de la fourniture d'accès internet est très différent du marché chinois. Avant sa révision en 2011⁸³⁹ annonciatrice du tournant de 2012, la loi sur les médias de 1991 votée sous le mandat de Boris Eltsine suivait une logique libérale : en reconnaissant le droit des fournisseurs d'accès internet et de services de publication en ligne à fournir librement leurs prestations sur le marché russe sous la qualification légale de « média de masse » ; en limitant le nombre de contenus censurés à trois catégories d'informations spécialisées (commission d'actes criminels en ligne, divulgation de secrets d'État, diffusion, incitation ou promotion en ligne d'activités terroristes) ; et en conditionnant toute censure par une décision de justice. Ce cadre légal confiait l'essor du marché à des initiatives privées, et tenait l'autorité administrative à l'écart de ce développement. Contrairement à la Chine, une myriade d'opérateurs privés a émergé sur le

services de communication télématique, 10 sept. 2007, art. I). Le cybercafé rentre dans ce champ puisqu'il fournit à des abonnés la possibilité de produire des datagrammes IP (informations structurées selon le protocole IP) depuis les machines qu'il met à disposition.

836 Réponse du Ministre du développement numérique, des communications et des médias de masse de la Fédération de Russie à la question citoyenne « Comment s'effectue l'identification des utilisateurs de services de communication, et qui l'effectue ? », sur *Ministère du développement numérique, des communications et des médias de masse* [en ligne], déc. 2017 (question posée : « Как осуществляется идентификация пользователей услугами связи, и кто ее осуществляет? ») ; et ANTIPOV Alexander, « Ministère des Communications : l'identification des utilisateurs du Wi-Fi n'est pas de la responsabilité des restaurateurs » [en ligne], sur *Security Lab Ru*, 22 décembre 2017 (« Минкомсвязи: Идентификация пользователей Wi-Fi не входит в обязанности рестораторов »).

837 Loi fédérale de 2003 sur les communications, art. 34§1, 4)

838 Roskomnadzor, *Mémo pour les personnes morales et les entrepreneurs individuels qui organisent l'accès au réseau d'information et de télécommunication Internet via des réseaux Wi-Fi publics* [en ligne], avr. 2020 (Памятка для юридических лиц и индивидуальных предпринимателей, организующих доступ к информационно-телекоммуникационной сети Интернет посредством общедоступных Wi-Fi сетей) [consulté le 26 août 2022].

839 Loi fédérale n 142-FZ du 14 juin 2011 portant modification de certains textes de loi de la Fédération de Russie en vue d'améliorer la législation applicable au secteur de l'information de masse » (Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового регулирования в сфере средств массовой информации"). Cette révision prépare le terrain d'une régulation par restriction du réseau russe à l'échelle de tous ses acteurs. Elle définit toute « publication en ligne » comme une catégorie de média de masse, et impose à tout propriétaire de site(s) internet l'obligation de s'enregistrer auprès du Roskomnadzor avant de fournir ses services sur le réseau russe.

marché russe par manque d'investissement public⁸⁴⁰. Face à l'hétérogénéité du territoire russe, chaque opérateur s'est déployé dans la ou les régions les plus rentables pour lui, de façon que le réseau national est en fait une interconnexion (par *peering*) de divers réseaux régionaux ou inter-régionaux concurrentiels⁸⁴¹. En contraste avec la Chine, l'État fédéral de Russie exerce donc un moindre contrôle économique sur les décisions et actions des multiples opérateurs détenteurs d'une licence : « *une véritable défiance s'est installée vis-à-vis des autorités, tandis que les opérateurs sont depuis longtemps rompus à la pratique d'une certaine « résistance passive » vis-à-vis des injonctions de surveillance numérique du pouvoir (Ermoshina et Musiani, 2017). (...) Certains opérateurs ont pu confier sous couvert d'anonymat qu'ils n'hésitaient pas à "faire tomber malencontreusement le matériel [de DPI] à sa réception" (Sanz-Pascual, 2020).* »⁸⁴². L'éparpillement des opérateurs et leur indépendance économique vis-à-vis de l'État empêchent le système russe de filtrage des candidats à la fourniture d'accès internet de déboucher sur une restriction cohérente des contenus illicites.

La plupart des États restreint le droit de fournir un accès internet par des mécanismes de certificats, de licences, d'autorisations... ne serait-ce que pour la fourniture d'un accès internet par voie hertzienne. Cette restriction de la fourniture par voie hertzienne s'explique par le fait que les fréquences hertziennes ne sont pas une ressource illimitée : elles résultent de charges électriques qui génèrent des ondes électromagnétiques, de façon que les fréquences disponibles sont proportionnelles à l'énergie électrique produite. Le spectre hertzien est donc limité par l'énergie électrique que les sociétés humaines peuvent produire, économiquement, dans le temps et dans l'environnement. Pour cette raison, la totalité des États a reconnu à une organisation internationale – l'Union internationale des télécommunications (UIT) – l'arbitrage de la répartition entre les États de cette ressource à la fois limitée et mondialement disponible. L'UIT alloue aux États les portions du spectre électromagnétique disponible dans le monde⁸⁴³, et les États régulent sur leur propre territoire la portion allouée par l'UIT (par ex., en autorisant ou en interdisant telle exploitation de telle fréquence). Propriétés des États, les fréquences hertziennes sont exploitables dans les conditions fixées par chaque État.

On étudie dans un même bloc le filtrage des candidats à la fourniture d'accès internet aux États-Unis et au Royaume-Uni, tant leurs régimes juridiques se ressemblent sur ce point. Dans les deux cas, seuls les opérateurs qui exploitent directement les fréquences hertziennes doivent

840LIMONIER Kevin, « Vers un « Runet souverain » ? » [en ligne], *EchoGéo* n° 56, Pôle de recherche pour l'organisation et la diffusion de l'information géographique (CNRS UMR 8586), août 2021, §29 : « *un rapport de la Cour fédérale des comptes de 2015 estimait qu'il existait dans le pays 15 433 entreprises détenant une licence (...) [bien que] toutes ces licences ne [soient] probablement pas utilisées (...) Aux États-Unis, où la gestion des télécoms est historiquement moins marquée par l'interventionnisme de l'État, on compte (...) un [FAI] pour 120 000 habitants environ. En Russie, ce ratio descend à un FAI pour 9 330 habitants.* »

841Ibid., §31 : « *la taille du territoire a également été un facteur important : de nombreuses villes éloignées des grands axes de communication n'intéressaient pas les quelques grands opérateurs russes, car trop chères à connecter pour si peu d'abonnés potentiels. De fait, une foule d'initiatives "par le bas" sont venues pallier ces difficultés – donnant naissance à une quantité de petits opérateurs aujourd'hui bien implantés, ainsi qu'à des pratiques numériques tout à fait singulières (Kolozaridi et Muravyov, 2020).* »

⁸⁴² Ibid., §34

⁸⁴³Convention internationale des télécommunications de 1959, art. 4, §2, a) et b)

obtenir une licence, auprès de l'Ofcom au Royaume-Uni⁸⁴⁴ ou de la FCC aux États-Unis⁸⁴⁵. Ce champ couvre les opérateurs téléphoniques, satellitaires, aéronautiques (fourniture d'internet dans les avions) etc. Pour l'essentiel, l'acquisition d'une licence contraint ces opérateurs à posséder des équipements autorisés par l'Ofcom ou par la *Civil Aviation Authority* au Royaume-Uni⁸⁴⁶, ou autorisés par la FCC aux États-Unis⁸⁴⁷, à respecter le droit national et international sur la régulation des fréquences hertziennes, à subir potentiellement des inspections de l'Ofcom ou de la FCC auprès des équipements voire la mise hors-tension des équipements... En revanche, n'est soumise à l'obtention d'aucune licence la personne qui n'exploite pas directement les fréquences hertziennes. Ce champ inclut donc les personnes qui les exploitent indirectement. Dans le domaine du réseau internet, cette exemption de licence concerne deux types de FAI exploitant indirectement les ondes hertziennes.

Premièrement, certains FAI fournissent un réseau local sans-fil : de nombreux restaurants, cafés, hôtels, magasins et autres entreprises peuvent offrir à leurs clients et salariés un point d'accès Wi-Fi à internet. Dans de telles situations, si ces entreprises fournissent elles-mêmes le service, elles doivent s'équiper d'un matériel Wi-Fi (de type borne) conforme aux normes techniques⁸⁴⁸. Cependant, pour que leur réseau Wi-Fi puisse donner un accès mondial à internet, ces petits FAI doivent connecter leur équipement à celui d'un opérateur de grande taille (de type Tier 1), dont le réseau est vastement déployé et connecté à d'autres grands réseaux. Ces fournisseurs de réseaux locaux sans fil peuvent donc exploiter les ondes hertziennes seulement dans la mesure du spectre que leur loue le grand opérateur auquel ils se connectent, lequel puise dans le spectre total que lui attribue la licence. Dès lors, ces petits FAI sans fil exploitent indirectement les ondes hertziennes – par le biais et par location du spectre d'opérateurs licenciés –, et ne requièrent aucune licence. En janvier 2020, l'Ofcom élargit la bande exploitable pour le Wi-Fi sans licence, autorisant ces réseaux locaux sans fil à exploiter non plus seulement la bande 5 GHz mais aussi désormais la bande 6 GHz (5925-6425 MHz), pourvu que les équipements utilisés soient conformes aux normes techniques⁸⁴⁹. Dans les faits, cet élargissement ouvre davantage le marché des fournisseurs d'accès internet par Wi-Fi de petite taille en les exemptant de toute licence sur une fréquence plus vaste, et leur permet d'accélérer le débit de leur trafic. Quatre mois plus tard, la FCC emboîte le pas de l'Ofcom, en prenant la

844 *Wireless Telegraphy Act* du 8 nov. 2006

845 *Communications Act* du 19 juin 1934, art. 307 et 331

846 Ofcom, *Wireless Telegraphy Act Licensing. Terms, Provisions and Limitations* [en ligne], 2011. L'Ofcom établit neuf grandes catégories de licences selon le mode de transmission (aéronautique, maritime, satellitaire, radiodiffusion...) et la qualification du fournisseur (amateur, radio-commerce...).

847 Code of Federal Regulations, Title 47, Part 2 (« Frequency allocation and radio treaty matters; general rules and regulations »)

848 Au Royaume-Uni, v. Ofcom, *Interface Requirements IR 2030 – Licence Exempt Short Range Devices*, 2021 ; aux États-Unis, la FCC délègue à des laboratoires d'accréditation qui certifient les équipements mis sur le marché américain, v. FCC, *Equipment Authorization. Approval Guide* [en ligne], oct. 2015

849 Ainsi, les bornes qui exploitent la bande 6 GHz ne doivent pas émettre plus de 250 mW en intérieur et 25 mW en extérieur : Ofcom, *Improving spectrum access for Wi-Fi. Spectrum use in the 5 and 6 GHz bands*, janv. 2020

même décision d'élargir à la bande 6 GHz les fréquences exploitables pour le Wi-Fi sans licence, jusqu'alors réservées à la bande 5 GHz⁸⁵⁰.

Deuxièmement, certains FAI fournissent un réseau filaire non hertzien (*i.e.* par câbles hors fibre optique). Cela concerne de petits voire moyens opérateurs (de type Tier 3 voire Tier 2) qui fournissent localement ou régionalement un réseau. Il peut s'agir d'une personne désireuse d'être son propre opérateur, ou d'une société qui propose à ses abonnés l'installation de câbles les reliant aux équipements de la société. Dans les deux cas, si cette personne ou cette société ne veut pas ou ne peut pas déployer son propre réseau à grande échelle, elle doit *in fine* raccorder ses équipements à ceux de grands opérateurs pour fournir un accès à l'internet national ou international. Tant cette personne que cette société fournissent un accès internet en exploitant indirectement les ondes hertziennes, du fait de leur raccordement au réseau d'un grand opérateur équipé d'infrastructures de transmission hertzienne longue portée. Dès lors, ne requièrent de licence de la part de l'Ofcom ou de la FCC ni les entreprises qui fournissent un accès local sans-fil (y compris les cybercafés), ni les personnes qui fournissent un accès exclusivement filaire, ni les sociétés ou communautés locales qui combinent un accès filaire avec l'utilisation de bornes Wi-Fi pour étendre leur réseau. En Chine et en Russie, les personnes qui fournissent un accès exclusivement filaire à des abonnés ou les sociétés et communautés qui combinent accès filaire et accès sans-fil sont qualifiables d'opérateurs de fourniture d'accès internet, à ce titre soumis aux licences pertinentes.

Ce système sans licence ne doit pas tromper sur ses conséquences potentiellement restrictives de l'accès au réseau. En effet, tout nouvel entrant sur le marché de la fourniture d'accès internet doit passer des contrats de *peering* avec les grands opérateurs pour établir un point d'échange avec le réseau international. Or, les nouveaux entrants sont généralement des opérateurs Tier 3 ou Tier 2 dans une position très nettement inférieure sur le marché par rapport aux grands opérateurs – à moins d'avoir les moyens financiers pour construire leur réseau à grande échelle en installant des infrastructures de transmission hertzienne longue portée (privilège généralement réservé à de grands opérateurs étrangers ou groupes industriels ou déjà implantés sur d'autres marchés) et d'obtenir une licence à cette fin. Au Royaume-Uni et aux États-Unis, le filtrage des nouveaux entrants sur le marché des FAI résulte moins des licences (sauf pour les grands opérateurs) que d'une hiérarchie contractuelle de type « pyramide » avec, à sa base, les plus petits opérateurs (Tier 3 et 2) qui doivent obéir aux règles établies par les plus grands (Tier 1) au sommet⁸⁵¹ – comparable à la pyramide contractuelle qui lie les *registry* et *registrar* à l'Icann. Presque tous les nouveaux entrants sur le marché peuvent donc fournir un service d'accès internet s'ils acceptent et se conforment aux conditions de gestion du trafic exigées par le grand

850FCC, *Unlicensed Use of the 6 GHz Band; Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz*, FCC-20-51, avr. 2020

851 Sur la domination du marché par les grands opérateurs (notamment téléphoniques) au moyen de l'instrument concurrentiel : au Royaume-Uni, v. VAN GORP Annemijn F., MAITLAND Carleen F. et HANEKOP Heidemarie, « The broadband Internet access market », *Telecommunications Policy*, vol. 30, 2006 ; aux États-Unis, v. UPPALURI Anusha, *A Two-market Inter-ISP Contracting Framework*, Thèse d'informatique, UMI, 2011 et FU Chuan, ZHANG Guoqing, YANG Jing et LIU Xiaona, « Study on the contract characteristics of Internet architecture », *Enterprise Information Systems*, vol. 5, Taylor & Francis, 2011, p. 495-513

opérateur en position dominante auquel ils se connectent⁸⁵². Or, on a vu que les règles de gestion du trafic divergent fortement entre le Royaume-Uni et les États-Unis. Au Royaume-Uni où tous les grands opérateurs emploient des systèmes de blocage voire de filtrage par défaut, les contrats de *peering* passés avec des Tier 3 et 2 comportent probablement l'interdiction faite au petit ou moyen opérateur d'entraver le bon fonctionnement de ces systèmes. Par ailleurs, tant au Royaume-Uni qu'aux États-Unis, on a relevé que les politiques de gestion du trafic sont assez librement fixées par les grands opérateurs – plus encore aux États-Unis où aucun principe de neutralité d'internet n'est consacré à l'échelon fédéral. Par conséquent, les petits et moyens opérateurs peuvent se voir imposer des règles de gestion de trafic variables voire contraires d'un grand opérateur à un autre. Bien plus que les licences, ce sont donc ici les lois économiques du marché⁸⁵³ et les stipulations contractuelles qui déterminent les critères pour filtrer les candidats à la fourniture d'accès à internet dans le cadre d'une pyramide contractuelle.

En Chine et en Russie, les candidats pour la fourniture d'un service d'accès à internet sont principalement filtrés par l'administration. Au Royaume-Uni et aux États-Unis, les candidats sont libérés de l'administration mais leur sélection est assujettie aux contrats des grands opérateurs et aux lois du marché. Quant à la France, on étudiera son cas un peu plus loin, à l'occasion de l'examen de la régulation par augmentation de l'accès.

Paragraphe 2 – Le filtrage du stockage de données

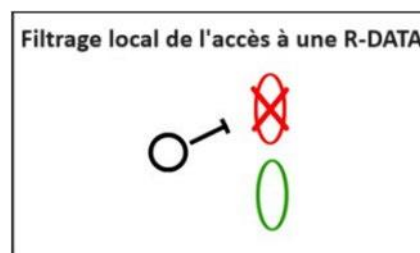
Au stade de leur stockage, les données peuvent être filtrées localement (A) ou en ligne. Dans ce dernier cas, le filtrage peut être automatisé ou manuel (B), et on étudiera les cas où le filtrage pratiqué depuis un serveur cible des contenus (C).

⁸⁵² La voie classique d'intégration sur le marché des FAI consiste souscrire des contrats de *peering* avec les grands opérateurs : v. l'article publié par le site britannique Startups.co.uk (4,8 millions d'utilisateurs uniques) de conseil aux entreprises britanniques naissantes, WATTS Julia, « How to become an internet service provider (ISP) | Guide by Startups.co.uk », sur *Startups.co.uk* [en ligne], publié le 3 mai 2018, [consulté le 23 août 2022]. ; v. aussi l'article publié par le site de comparaison du marché technologique, STURT Robert, « How to become an ISP via BT? », sur *Netify.com*, 10 oct. 2019

⁸⁵³ Ainsi, au Royaume-Uni, les zones territoriales délaissées par les grands opérateurs (car peu rentables par rapport à l'environnement local, au nombre de personnes desservies, aux obligations contractuelles existantes...) sont de plus en plus couvertes par les « *fournisseurs alternatifs* » (services publics, communautés locales) sous l'effet d'une compétition entre ces derniers sur un marché de niche (marché très étroit, resserré sur un bien ou service très spécialisé). Les lois économiques sont donc le moyen par lequel progresse la couverture numérique du territoire au Royaume-Uni. V. GERLI Paolo, WAINWRIGHT David et WHALLEY Jason, « Infrastructure investment on the margins of the market », *Telecommunications Policy*, 41, 2017.

A) Techniques de filtrage local

La configuration est la même que pour le filtrage local dès l'acheminement, mais le nœud émetteur qui pratique le filtrage est cette fois incarné par un terminal – au lieu d'un routeur. Le filtrage local opère dans ce cas en empêchant le terminal de produire une requête. C'est par exemple le cas des logiciels antivirus qui empêchent l'utilisateur de télécharger un fichier suspect ou manifestement malveillant. On étudiera quatre techniques de filtrage local instrumentalisées par les États.



• Le filtrage par restriction d'accès à un terminal

Cette première technique de filtrage dès le stockage consiste à limiter la possibilité même d'utiliser un terminal. On examine deux exploitations étatiques de cette technique : le cas nord-coréen ; et les prisons françaises.

Du côté de la Corée du Nord, dès le développement des premiers ordinateurs sur le territoire nord-coréen dans les années 1990-2000, l'État a conditionné l'acquisition d'un ordinateur personnel par la délivrance d'une autorisation administrative⁸⁵⁴. Faute de moyens financiers suffisants ou d'une autorisation administrative, les citoyens Nord-coréens qui utilisaient un ordinateur dans les années 2000 y accédaient principalement dans des salles d'ordinateurs collectifs (bibliothèques, cybercafés...) où chaque utilisateur, éduqué à la délation, peut surveiller l'activité des autres utilisateurs ou craindre d'être surveillé par autrui⁸⁵⁵. À l'exception des touristes, des ambassades et de l'élite comme on le verra, les nord-coréens ne peuvent accéder qu'à un réseau fermé sur lui-même, baptisé « Kwangmyong » (Lumière)⁸⁵⁶. Une première méthode employée par la Corée du Nord pour filtrer l'accès à internet réside donc dans le fait de conditionner l'acquisition d'un ordinateur personnel par l'obtention d'une autorisation administrative. Il semble toutefois que, depuis la deuxième moitié des années 2010, les Nord-coréens privilégient l'accès à internet au moyen de smartphones plutôt que d'ordinateurs⁸⁵⁷, et le phénomène ne cesse de croître. D'après le groupe américain de réflexion et d'investigation 38 North, consacré à l'analyse de la Corée du Nord, entre 6,5 et 7 millions de nord-coréens

⁸⁵⁴ BOYNTON Robert S., « North Korea's Digital Underground » [en ligne], *The Atlantic*, avr. 2011

⁸⁵⁵ LEE Jong-Heon, « Internet cafe opens in N.Korea », *United Press International*, 28 mai 2002. V. aussi « North Korea: Connection Denied » [en ligne], préc., *Amnesty International*, 2016, p. 19.

⁸⁵⁶ En 2016, un journaliste de l'Yle (journal finlandais) se rend en Corée du Nord, d'où il accède au réseau Kwangmyong depuis la salle informatique de l'usine de soie de Pyongyang. Il filme sa navigation sur Kwangmyong, partage la vidéo sur le site yle.fi, et recense au moins 91 sites web (principalement des sites web gouvernementaux, d'instituts de recherche, d'universités, de bibliothèques, d'industries et de services administratifs, de l'Agence centrale de presse coréenne ou encore de l'Association coréenne de cuisine : MÄKELÄINEN Mika, « Yle Pohjois-Koreassa: Kurkista suljetun maan omaan tietoverkkoon », *Yle*, 14 mai 2016. On expliquera plus loin comment la Corée du Nord a réussi à isoler le Kwangmyong du reste d'internet.

⁸⁵⁷ KIM Jaewon, « North Koreans tap into smartphone apps on restricted state network » [en ligne], *Nikkei*, 6 juin 2019

possédaient un smartphone en 2022 (soit plus de 25% de la population nationale) contre 3,8 millions en 2017⁸⁵⁸.

Outre le cas de la Corée du Nord, un filtrage dès le terminal est également pratiqué dans les prisons françaises. En France, l'accès à internet dans les prisons est interdit depuis une note de l'administration pénitentiaire du 21 mai 2004⁸⁵⁹. Une circulaire du 13 octobre 2009 rappelle l'interdiction absolue (*i.e.* ne souffrant aucune exception) des détenus d'accéder à internet :

« *l'échange ou la communication par un détenu de tout support informatique avec l'extérieur est strictement interdit* » et « *la remise de matériel informatique est prohibée aux parloirs* »⁸⁶⁰.

Cela exclut de fait la possession par un détenu d'un smartphone, qui fournit une connexion internet. De même, les ordinateurs mis à disposition des détenus en salle d'activité (bibliothèques, salles de formation, ateliers de travail, services généraux assurés par des détenus, salles d'activités socioculturelles et salles d'activités audiovisuelles) ne doivent offrir aucune « *connexion à des réseaux externes* »⁸⁶¹. Les ordinateurs présents en salle d'activité doivent offrir aux détenus des logiciels de numérisation graphique, de création multimédia ou audiovisuelle ou encore des outils bureautiques (logiciel de traitement de texte, tableur, logiciel de présentation, de traduction...) lorsque ces logiciels sont utiles voire nécessaires aux activités de formation et de travail des détenus⁸⁶². Les ordinateurs en salle d'activités sont programmés avec un mot de passe administrateur au niveau du BIOS (programme le plus basique d'un ordinateur, stocké par une puce insérée sur la carte-mère, qui sert à solliciter les différents composants matériels de l'ordinateur et à appeler les instructions appropriées pour le bon fonctionnement de la machine)⁸⁶³. Les détenus n'ayant pas connaissance de ce mot de passe, ils ne jouissent pas des droits d'administrateur local sur les ordinateurs en salle d'activité (impossibilité de télécharger des fichiers ou des applications, de supprimer des applications de bureau ou des dossiers...).

Les seuls appareils informatiques que les détenus peuvent acquérir en qualité de propriétaires au cours de leur détention doivent être délivrés par des « *fournisseurs agréés* » en vertu de conventions passées entre les établissements pénitentiaires et les fournisseurs de matériels informatiques locaux, régionaux ou nationaux. Là encore, il est interdit à ces fournisseurs de vendre aux détenus des matériels informatiques qui leur permettraient de communiquer avec l'extérieur⁸⁶⁴. Chaque détenu n'a droit qu'à un unique ordinateur et à un unique type de périphérique ; il ne peut utiliser que des disquettes pour transférer des données hors de son ordinateur, et il est autorisé à posséder des CD-ROM et DVD-ROM seulement s'ils sont marqués par l'administration pénitentiaire de façon à vérifier que les disques n'ont pas subi de modification de la part du détenu⁸⁶⁵. Dans le même sens, tout ordinateur personnel et tout ordinateur présent en salle d'activité doit se voir greffer un scellé de sécurité⁸⁶⁶. Ce scellé prend la forme d'un boîtier, que le détenu n'a le droit d'ouvrir en aucune circonstance. Les scellés

858KO Donghwan, « North Korea's 7 million smartphone users under regime's watchful eye » [en ligne], *The Korea Times*, nov. 2022

859Note du 21 mai 2004 intitulée Interdiction faite aux détenus d'accéder à internet et à tout [système d'information (SI)] extérieur

860Circulaire de la Direction de l'Administration pénitentiaire relative à l'accès à l'informatique pour les personnes placées sous main de justice du 13 octobre 2009, NOR : JUSK094006C, art. 2.3.2

861Ibid., art. 4.7

862Ibid., art. 4.1

863Ibid., art. 4.6

⁸⁶⁴ Ibid., art. 3.1.2

865Ibid., art. 3.2 et 3.3

866Ibid., art. 3.4 et 4.4

posés par l'administration pénitentiaire sont inventoriés de manière qu'à chaque scellé corresponde le nom du propriétaire de l'ordinateur, la date de pose du scellé et la personne de l'administration pénitentiaire ayant effectué la pose. Ce mécanisme permet à l'administration pénitentiaire de s'assurer que les ordinateurs n'ont pas été changés ni ouverts par les détenus. Enfin, le détenu doit communiquer à l'administration pénitentiaire ses mots de passe et identifiants d'accès à l'ordinateur pour permettre à celle-ci de vérifier le contenu du disque dur de l'ordinateur du détenu⁸⁶⁷. Dans ces conditions, tout accès à internet effectué pour le compte d'un détenu ne peut l'être que par son agent de probation, s'il en a le temps (pour des démarches comme la désinscription de Pôle Emploi ou de la Caisse d'allocations familiales, les virements bancaires etc.)⁸⁶⁸.

En pratique, ces mesures n'ont jamais été efficaces pour priver les détenus d'un accès internet. En 2012 déjà, une enquête journalistique du Monde révèle que les gardiens de prison ne parviennent pas à empêcher la pénétration des téléphones mobile dans l'enceinte des prisons : les parloirs « *seraient de vraies passoires. Les détenus dissimulent le boîtier dans leur pli fessier, la puce dans leur bouche, et réintègre leur cellule* »⁸⁶⁹. Ils cachaient ensuite le téléphone dans les « *blocs de WC, boîtes de conserve ou de sel* », voire « *les [scotchent] dans les portes de frigo, dans les matériaux d'isolation* », et fabriquaient des chargeurs de téléphone à partir de « *chargeurs de tondeuses pour cheveux sur lesquels les plus bricoleurs greffent un embout compatible avec leur téléphone* ». D'après un membre du Syndicat pénitentiaire des surveillants, « *aucun établissement n'est épargné [en 2012], c'est un véritable fléau* ». Le journaliste Arthur Frayer, qui a passé plusieurs mois dans les maisons d'arrêt de Fleury-Merogis et d'Orléans en tant que gardien de prison en 2011, confirmait que les parloirs étaient le lieu privilégié pour l'acquisition illicite de téléphones d'après son expérience personnelle, et rapportait que les téléphones portables pénétraient aussi dans l'enceinte des prisons « *grâce à la corruption des surveillants* » ou en étant « *projetés au-dessus du mur du centre par des complices* »⁸⁷⁰. Le phénomène ne s'est pas atténué depuis. En 2017, deux détenus de la prison de Fresnes estimaient que l'immense majorité des détenus utilisait des smartphones⁸⁷¹. Avi Bitton, avocat pénaliste au barreau de Paris, considère en 2021 que « *la pratique est répandue* » : « *il est fréquent que les avocats pénalistes reçoivent des appels de la prison depuis un téléphone portable* »⁸⁷². Au nombre des applications les plus populaires chez les détenus français, on trouve notamment les réseaux sociaux Snapchat ou encore TikTok – l'utilisateur de TikTok portant le pseudonyme « le Pingouin » est un détenu qui cumulait ainsi plus de 123 000 abonnés en décembre 2022⁸⁷³.

⁸⁶⁷*Ibid.*, art. 3.6

⁸⁶⁸Observatoire international des prisons, « Fracture numérique : les prisons, une "zone blanche" » [en ligne], *Revue Dedans-Dehors*, n° 113, déc. 2021

⁸⁶⁹« Le portable en prison : mobile d'évasion », *M le magazine du Monde*, sept. 2012

⁸⁷⁰TÔN Emilie, « Prison: "Presque chaque détenu possède un portable, certains en ont plusieurs" », *L'Express*, 2016

⁸⁷¹CONDOMINES Anaïs, « On a discuté avec des détenus sur Facebook : "Toute la taule a un smartphone" », sur *TF1info.fr*, oct. 2017

⁸⁷²REGNY Diane, « Détenus sur TikTok : que risquent ceux qui utilisent un téléphone portable en prison ? », *BFMTV*, déc. 2021

⁸⁷³DE PASQUALE Anthony, « Les prisonniers français sont sur Snapchat », sur *Vice.com*, fév. 2016 ; « Des détenus se filment sur Snapchat fumant un joint », *La Dépêche*, juil. 2018 ; « Béziers: des détenus mettent une annonce sur Snapchat pour trouver des "jeteurs" », *Le Figaro*, juil. 2019 ; RICHARD Julie, « TikTok s'infiltré en prison sans toquer à la porte », *Libération*, déc. 2022

● ***Le filtrage local par chiffrement de données***

On appelle « filtrage local par chiffrement de données » la technique qui consiste, depuis le terminal de l'utilisateur, à chiffrer ses données pour l'empêcher de produire ou stocker une R-DATA. On a déjà vu l'exemple de la Corée du Nord qui, depuis 2014, attribue une signature électronique à chacun de ses terminaux via leur système d'exploitation et une autre signature électronique aux services en ligne agréés par l'État. Identifié par sa signature dès son système d'exploitation, l'utilisateur d'un terminal nord-coréen ne peut ainsi accéder qu'aux applications certifiées par l'État. Les R-DATA ici filtrées sont la R-DATA « accès à des services en ligne étrangers » et « accès à des services en ligne non approuvés par l'État ». On renvoie à notre partie sur le chiffrement pour les détails de cette méthode [supra].

● ***Le filtrage local par pré-installation de logiciels***

On appelle « filtrage local par pré-installation de logiciels » la technique qui consiste à installer des programmes dès la fabrication du terminal pour empêcher l'utilisateur de produire ou stocker une R-DATA. Parmi les États qui exploitent cette technique, on retrouve à nouveau la Corée du Nord.

L'État nord-coréen exploite cette technique pour filtrer les transmissions de données par Wifi. En 2014, le gouvernement de la Corée du Nord désire mettre un terme à une pratique de certains Nord-coréens, qui consistait à capter les signaux électriques émis par les ambassades et ONG afin de se connecter à leur réseau wifi ou satellitaire et d'accéder à l'internet étranger⁸⁷⁴. En réponse à cette pratique, le Département national de la réglementation des radiocommunications publie en août 2014 un décret qui interdit aux « *missions diplomatiques et organisations internationales* » (ambassades et ONG) d'utiliser un réseau wifi ou satellitaire dans l'enceinte de leurs locaux sans avoir préalablement obtenu une licence de la part du Département⁸⁷⁵. Les licences semblent être destinées à pratiquer une coupure entre les machines situées dans les locaux concernés, et les machines des Nord-coréens⁸⁷⁶. Des Nord-coréens se sont à nouveau affranchis de cette restriction, en captant les signaux électriques émis par les smartphones des étrangers pour se connecter à leur réseau wifi – à leur arrivée en Corée du Nord, les étrangers se voient distribuer une carte SIM qui leur permet d'accéder à l'internet étranger. Quelques temps après, on ne sait exactement à quelle date, les Nord-coréens perdent la possibilité d'accéder à un quelconque réseau wifi sur tout le territoire⁸⁷⁷, ce qui contraint les signaux électriques en Corée à du Nord à n'emprunter que le réseau terrestre faute de réseau sous-marin, aérien et satellitaire. En 2018, le gouvernement rétablit sur le territoire un réseau wifi appelé Mirae (미래, « Avenir »), qui est un réseau wifi spécifiquement fermé sur les seuls appareils nord-coréens. À cette fin, chaque téléphone nord-coréen est équipé d'une carte SIM

⁸⁷⁴ « North Korea slaps Wi-Fi ban on embassies and NGOs » [en ligne], *The Korea Times*, 11 sept. 2014

⁸⁷⁵ Le motif avancé dans le décret tient à ce que le e transport aérien de signaux électriques produiraient « *un certain effet sur l'environnement* », v.« North Korea bans WiFi networks for foreigners | NK News », sur *NK News - North Korea News* [en ligne], publié le 8 septembre 2014, [consulté le 15 août 2022].

⁸⁷⁶ KECK Zachary, « North Korea Bans Wi-Fi for Foreigners », *The Diplomat*, 11 sept. 2014

⁸⁷⁷ « Selfies and surveillance: North Korea's new connectivity » [en ligne], *Bangkok Post*, 10 novembre 2017

programmée de façon à authentifier la provenance nord-coréenne de l'appareil⁸⁷⁸. Le réseau wifi Mirae ne peut transporter que les données qui contiennent cette authentification par SIM. De cette manière, les bornes wifi Mirae permettent uniquement aux appareils nord-coréens d'accéder à d'autres appareils nord-coréens. Ce triple filtrage sur terminaux (pour l'accès à un ordinateur, pour l'accès à des services non certifiés par l'État et pour l'accès au réseau Wifi) est complété par une surveillance de l'activité des utilisateurs, au moyen du logiciel d'État préinstallé Trace Viewer (ou History Viewer, 열람리력) qui effectue automatiquement des captures d'écran à intervalles réguliers pour inspecter les actions des utilisateurs⁸⁷⁹.

Outre la Corée du Nord, de nombreux États affichent un intérêt grandissant pour le filtrage local par pré-installation de logiciels à l'encontre d'une R-DATA spécifique : l'accès aux contenus pornographiques. Aux États-Unis, cette option fait de plus en plus d'adeptes parmi les États conservateurs. Ainsi le gouverneur de l'Utah a-t-il promulgué le 23 mars 2021 un amendement sanctionnant le fabricant qui autorise la vente ou la mise à disposition, sur le territoire de cet État, de tablettes ou de smartphones dont les logiciels préinstallés ne filtrent pas l'accès aux contenus pornographiques – toutes catégories d'âge confondues⁸⁸⁰. Si l'Utah est le premier État à établir un tel mécanisme de filtrage, « *d'autres États ont suivi l'exemple de l'Utah (...) – une douzaine d'États a présenté des résolutions similaires visant à déclarer la pornographie comme une crise de santé publique après que [l'Utah] fut le premier à le faire en 2016* »⁸⁸¹. Le 4 mai 2022, entre en vigueur une nouvelle loi de l'Utah qui impose la même obligation de filtrage des contenus pornographiques aux fabricants des terminaux fournis dans les écoles⁸⁸². La même année, de l'autre côté de l'Atlantique, la loi française oblige le fabricant de terminaux : à s'assurer que ses équipements comportent un dispositif de contrôle parental (par ex. en le vérifiant auprès du fournisseur du système d'exploitation) ; et à certifier aux importateurs, distributeurs et prestataires de services d'exécution des demandes que les terminaux mis sur le marché français comportent effectivement ce dispositif (lesquels importateurs, distributeurs et prestataires sont à leur tour tenus de vérifier la certification)⁸⁸³.

• La désactivation d'une fonction par filtrage

On a vu qu'une fonction logicielle peut être désactivée par suppression des données qui la constituent ou encore par blocage de l'accès à ces données depuis des serveurs. Une fonction peut aussi être désactivée par filtrage des requêtes de l'utilisateur, auquel cas la censure de

878 WILLIAMS Martyn, « Digital Trenches. North Korea's Information Counter-Offensive » [en ligne], préc., *Committee for Human Rights in North Korea (HKRN)*, 2019, p. 37-38

879 *Ibid.*, p. 35 ; v. aussi JEONG Tae-Joo, « La Corée du Nord demande aux organisations de mettre à jour leurs applications... et vérifie également si des programmes de contournement sont installés » (北, 앱 업데이트 조직적 지시...우회 프로그램 설치 여부도 검열) [en ligne], *Daily NK*, 8 juil. 2022

880 *Device Filter Amendments*, H.B. 72, 23 mars 2021. Cet Amendement n'est pas effectif en raison de son art. 8 qui conditionne l'entrée en vigueur de cet amendement par le fait que « *au moins cinq États autres que l'Utah adoptent une loi dans une forme substantiellement similaire* » [en ligne sur le site de l'Utah]

881 EPPOLITO Sophia et WHITEHURST Lindsay, « Utah campaign against porn marches on with phone filter plan », sur *Apnews.com*, 16 mars 2021

882 *Sensitive Materials in Shools*, H.B. 374, 24 mars 2022 [en ligne sur le site de l'Utah]

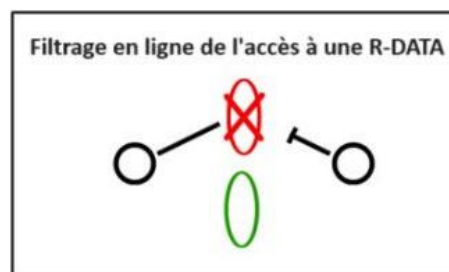
883 Loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet. Jusqu'à présent, les FAI étaient déjà obligés d'informer et de proposer à leurs abonnés un dispositif de contrôle parental (LCEN, art. 6, I, 1), mais aucune obligation de filtrage ne pesait sur le fabricant du terminal.

ladite fonction opère sur le terminal de l'utilisateur. Par exemple, la désactivation d'une fonction par filtrage a été récemment exploitée par l'État chinois. Quelques semaines avant les manifestations du 26 novembre au 7 décembre 2022 en Chine, dirigées contre la politique nationale de « zéro covid », Apple restreint l'une des fonctions proposée par les iPhone : la fonction AirDrop. Cette fonctionnalité, qui s'appuie sur les technologies Bluetooth et Wifi, permet aux utilisateurs d'iPhone de s'échanger des contenus à courte distance (moins de 5 mètres) par voie exclusivement hertzienne – donc sans emprunter le réseau des opérateurs sur une telle distance. Dans un contexte de manifestations populaires, cette fonction peut être utilisée pour diffuser auprès de millions de manifestants des contenus dont la transmission échappe au contrôle des opérateurs et de l'État. AirDrop avait ainsi été massivement employée par la manifestations hong-kongaises de 2019, et avait encore été exploité en octobre 2022 par un contestataire pour diffuser des messages d'opposition sur des bannières publiques⁸⁸⁴. Le 9 novembre 2022, Apple met à jour son système d'exploitation iOS, et restreint à cette occasion AirDrop pour les seuls iPhones vendus en Chine continentale. Concrètement, la fonctionnalité « envoi à tout le monde » se désactive automatiquement après 10 minutes d'utilisation, et les utilisateurs d'AirDrop seront alors contraints d'envoyer leurs messages à leurs seuls contacts ou de désactiver la fonction⁸⁸⁵. Compte tenu du contexte protestataire chinois, du passif d'AirDrop en Chine, de la date de la mise à jour d'AirDrop et de sa limitation au territoire chinois, on pense très probable que l'État chinois ait fait pression sur Apple afin de limiter la diffusion à grande échelle et incontrôlable de contenus protestataires.

B) Techniques de filtrage en ligne : comparaison des filtrages manuel et automatisé

La configuration est la même que pour le filtrage en ligne dès l'acheminement, mais le nœud récepteur qui pratique le filtrage est cette fois incarné par un serveur – au lieu d'un routeur. On a vu que le blocage consiste à empêcher l'utilisateur d'accéder à des données déjà hébergées sur internet (en jouant sur la destination de la requête), tandis que le filtrage en ligne consiste à empêcher l'utilisateur de produire des données porteuses de R-DATA (en jouant sur les autres caractéristiques de la

requête). Le filtrage en ligne offre ainsi la possibilité d'agir notamment sur les contenus d'information que porte une donnée. On appelle « contenu d'information » tout texte, image, vidéo ou son produit ou diffusé sur internet.



On relève par ailleurs que le filtrage dès le stockage de données, pratiqué au niveau du terminal (local) ou du serveur (en ligne), présente l'avantage d'être adapté contre les données qui sont hébergées durablement (contenus, applications, bases de données, fichiers...). À l'inverse, pratiqué au niveau du routeur, le filtrage dès l'acheminement de données peine aujourd'hui à filtrer de telles données sans ralentir l'accès à un service ou à un autre terminal (en raison du temps nécessaire à l'analyse des caractéristiques des données durant leur acheminement). Autrement dit, **le filtrage dès le stockage de données permet de filtrer les caractéristiques d'une requête sans affecter le**

⁸⁸⁴GILCHRIST Karen, « Apple limited a crucial AirDrop function in China just weeks before protests », *CNBC*, 30 nov. 2022

⁸⁸⁵*Ibid.*

trafic. Lorsqu'il est question de restreindre l'accès d'une requête d'après ses caractéristiques, il est donc préférable de filtrer les données depuis leur source de stockage (terminal, serveur et périphériques accessoires) plutôt que depuis leur source d'acheminement (routeur). Après avoir vu le filtrage sur terminal, on explore ici quatre exemple de filtrage sur serveur.

- **Le filtrage par fixation préalable du contenu (filtrage manuel du contenu)**

Parfois appelé « modération [humaine] *a priori* », le filtrage par fixation préalable des contenus consiste à mettre en attente les contenus qui appellent publication, et à n'en autoriser la publication qu'après avoir été examinés par un modérateur humain⁸⁸⁶. Les contenus sont ainsi « fixés » avant toute publication. Cette technique présente le double avantage : de couvrir la totalité des contenus publiés ; et de modérer un contenu avant qu'il puisse acquérir la moindre échelle de production ou de réalisation.

Elle est cependant très limitée par deux inconvénients de taille. D'une part, les contenus autorisés ou interdits le sont d'après l'interprétation du seul modérateur qui filtre ces contenus. La multitude de modérateurs et d'applications sur internet aggrave le manque d'homogénéité interprétative pour le filtrage de contenus, de sorte que le filtrage par fixation préalable peut aboutir à un résultat (contenus effectivement publiés sur chaque application) très différent de ce qu'exige la loi, surtout s'il est généralisé à de nombreuses applications⁸⁸⁷.

D'autre part, le filtrage par fixation préalable est très inadapté lorsque le service qui pratique le filtrage abrite une forte activité participative. Par exemple, chaque seconde, sont publiés plus 1 500 vidéos sur TikTok, 6 000 tweets, 8 500 commentaires sur Facebook, 15 000 images sur Instagram (dont 1 160 via des posts, et le reste via des stories et chats)⁸⁸⁸... Dès qu'un serveur héberge plus de 10 nouveaux contenus publics par seconde, il commence à devenir très difficile de pratiquer un filtrage par fixation préalable. À un tel rythme de 10 publications/seconde, 864 000 contenus sont publiés par jour. En supposant qu'un **modérateur travaille 10h/jour** (y compris les week-end), et **qu'il consacre en moyenne 5 secondes d'analyse à chaque contenu** avant d'en autoriser la publication, il lui faudrait 50 jours pour analyser les 864 000 contenus publiés en une seule journée. **Pour que la totalité des 864 000 contenus publiés/jour soit analysée et traitée en une seule journée, il faudrait une équipe de 120 modérateurs respectant le rythme de travail indiqué.** Si chaque modérateur a besoin en moyenne de 10 secondes d'analyse par contenu au lieu de 5, l'équipe devra être composée de 240 modérateurs pour pouvoir filtrer les contenus quasiment en temps réel. À ce même rythme d'analyse, si chaque modérateur travaille 10h/jour 6 jours sur 7, l'équipe devra être composée de 285 modérateurs.

⁸⁸⁶Le chercheur spécialisé en droit de la communication Emmanuel Derieux définit la fixation préalable comme « *tout procédé qui permet de prendre connaissance du message litigieux avant sa mise à disposition du public et, par conséquent, de s'y opposer* » (DERIEUX Emmanuel, « Responsabilité du "producteur" d'un service de communication au public en ligne : condition d'une fixation préalable », *La revue européenne des médias et du numérique*, n°20, automne 2011).

⁸⁸⁷On a déjà démontré que la démultiplication du nombre d'interprètes a pour effet d'altérer une règle $F \rightarrow C$ au moment de son application, cf. Partie I, Sous-Partie 2, Chapitre 2, Paragraphe 1

⁸⁸⁸On a calculé les chiffres de TikTok à partir du rapport de transparence de TikTok d'avril-juin 2022, qui indiquait alors que le nombre de vidéos produites sur ce trimestre était légèrement supérieur à 113 millions « Community Guidelines Enforcement Report Apr-Jun 2022 », sur *TikTok.com*, 28 sept. 2022 ; COËFFÉ Thomas, « Chiffres Twitter – 2022 », sur *Blogdumoderateur.com*, mis à jour le 1^{er} mars 2022 ; OSMAN Maddy, « Statistiques et faits intéressants sur Facebook (2023) », sur *Kinsta.com* [hébergeur cloud], 7 déc. 2022

À ce même rythme d'analyse et de travail, **l'équipe de modération d'Instagram devra être composée de 212 418 à 424 837 modérateurs exclusivement dédiés à cette tâche pour filtrer quasiment en temps réel la totalité des images publiées chaque jour sur Instagram** (sans compter les vidéos, commentaires et autres publications textuelles, les extraits audio...).

Il n'est pas possible de réunir des équipes de modération suffisamment nombreuses pour filtrer une très grande quantité de contenus. La modération *a priori* porte donc le même inconvénient que le filtrage des contenus dès l'acheminement : face à un afflux de requêtes, elle ralentit l'accès au service. Par conséquent, **le filtrage par fixation préalable est incompatible avec des applications dont les contenus sont issus d'une forte participation** comme les réseaux sociaux, les moteurs de recherche, les applications de partage de contenus pornographiques ou les places de marché.

En France, la loi a pour effet de décourager le recours au filtrage par fixation préalable. Venue modifier l'art. 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle pour l'adapter aux infractions de presse commises en ligne, la loi Hadopi du 12 juin 2009 pose un régime de responsabilité en cascade. Lorsqu'il y a eu fixation préalable, la responsabilité d'une infraction de presse incombe au directeur de publication (*i.e.* l'éditeur du site web) ou, à défaut, à l'auteur du contenu (l'internaute) ou, à défaut, au producteur (l'hébergeur). Le propriétaire du site web qui pratique un filtrage par fixation préalable est donc – avant l'utilisateur – responsable des infractions de presse commises par les utilisateurs de son application. Ce régime en cascade est la conséquence du régime européen déjà étudié de responsabilité des éditeurs (responsables par principe car exerçant un contrôle resserré sur les contenus) et des hébergeurs (irresponsables par principe car exerçant un contrôle distant sur les contenus). Les infractions de presse en ligne punies par le droit français, et pour lesquelles le propriétaire d'un site web peut être tenu responsable, concernent principalement les propos haineux⁸⁸⁹, les fausses informations et la contestation de crimes contre l'humanité. Pour s'éviter la responsabilité de tels contenus diffusés sur son site, le propriétaire d'un site web français a donc tout intérêt à ne pas pratiquer de fixation préalable.

Au contraire, en Chine, tous les fournisseurs de services en ligne sont responsables des contenus publiés, et cette responsabilité oblige certains d'entre eux à pratiquer un filtrage par fixation préalable. L'Administration du Cyberspace de la Chine (CAC) ordonne ainsi depuis 2017 un filtrage des contenus issus des commentaires en ligne : les prestataires de services de publication de commentaires doivent approuver, préalablement à toute publication, chaque commentaire (i) exprimé sous une actualité ou (ii) provenant de comptes inscrits sur une « *liste noire* » en raison de leur « *grave manque de fiabilité* » évalué notamment sur la base de leur « *crédit de publication* »⁸⁹⁰. En limitant ainsi le filtrage aux contenus de certains internautes seulement, et spécifiquement aux commentaires publiés sous des actualités, la loi réduit considérablement le volume de contenus à filtrer et rend ainsi possible le recours à la modération humaine *a priori* dans la majorité des cas.

889En droit français, les propos haineux couvrent les infractions de diffamation, d'injure et de provocation à la discrimination, à la haine ou à la violence à raison de l'appartenance ou non-appartenance de la personne diffamée à une ethnie/nation/race/religion (1^{er} groupe de motifs) ou de son sexe/orientation sexuelle/identité de genre/handicap (2^e groupe de motifs)

890CAC, Dispositions relatives à l'administration des services de commentaire sur internet (互联网跟贴评论服务管理规定), art. 5(3) et 9

Cependant, dans la mesure où cette modération humaine *a priori* est inadaptée aux services dont les contenus sont issus d'une forte participation, le droit chinois impose des conditions de travail très difficiles à tenir à long terme pour les modérateurs. Le magazine Sixth Tone, journal appartenant à l'État chinois, rapporte que « *beaucoup [de modérateurs] ont reçu un diagnostic de psychasthénie* » (incapacité à agir, absence d'attention, manque d'appétit, insomnie, obsessions, angoisses, doute permanent, ruminations, phobies et inhibitions) d'après un jeune homme de 24 ans examinateur de commentaires dans l'équipe de Kuaishou (application proche de Snapchat en Occident)⁸⁹¹. « *Mon cycle menstruel est devenu irrégulier. J'avais l'impression que mon cerveau s'arrêtait de fonctionner pendant les quarts de travail et que j'avais une vision floue, ce qui entraînait une augmentation des erreurs et donc une réduction de salaire* » déclare une modératrice de Bilibili (application proche de YouTube). Un autre modérateur, âgé de 26 ans et travaillant pour l'équipe de ByteDance (propriétaire des applications TikTok, Capcut et Toutiao), témoigne avoir « *pris 10 kilos en raison d'un mode de vie irrégulier en travaillant là-bas... Les nuits blanches sont si tortueuses que parfois, on a l'impression d'être sur le point de mourir.* ». Le 4 février 2022, âgé de 24 ans, un modérateur de Bilibili décède, apparemment en raison d'un épuisement professionnel : « *la mort de l'employé (...) a déclenché une vague de colère et de sympathie du public. Il a également donné un aperçu de la vie personnelle et professionnelle de dizaines de milliers de modérateurs de contenu* ». Fin 2020, l'équipe de Bilibili était composée de 2 400 modérateurs, et celle de ByteDance en comptait plus de 20 000 modérateurs. Les modérateurs chinois de contenus travaillent le plus souvent sous le régime des heures supplémentaires dit « 996 » (de 9h du matin à 9h du soir, six jours par semaine).

Compte tenu de la difficulté de sa mise en œuvre, la modération humaine *a priori* n'est pas la plus privilégiée par les États. En effet, depuis les années 2010, les États concentrent plutôt leur régulation sur des acteurs qui centralisent un grand nombre de contenus ce qui est difficilement compatible avec une modération humaine *a priori*. Cette préférence des États étudiés pour la régulation des acteurs centraux favorise des techniques automatisées de filtrage

• ***Le filtrage par reconnaissance algorithmique ou intelligente (filtrage automatisé du contenu)***

Le filtrage par reconnaissance algorithmique ou intelligente n'est autre qu'un filtrage *automatisé* par fixation préalable : les contenus qui appellent publication sont mis en attente, d'ici à ce que leur publication soit autorisée par un algorithme ou une intelligence artificielle (au lieu d'être autorisée par un être humain). Cette différence avec la modération humaine *a priori* est très importante, car l'automatisation lève les deux principaux inconvénients du filtrage par fixation préalable. D'une part, la disparité interprétative des modérateurs humains laisse place à une homogénéité par automatisation pour l'application des règles légales. Le filtrage n'obéit donc plus aux lois de l'interprétation (écart entre la règle $F \rightarrow C$ créée et la règle $F \rightarrow C$ appliquée) mais aux lois de l'interopérabilité (application à l'identique de la règle $F \rightarrow C$ créée), garantissant ainsi que les applications faites d'une règle sont conformes à cette règle telle qu'énoncée. En d'autres termes, par rapport à la modération *a priori*, **le filtrage automatisé assure une application beaucoup plus intégrée et homogène de la règle énoncée**. D'autre part, le temps d'analyse des contenus par un algorithme ou une IA est très nettement raccourci par rapport au temps d'analyse qu'y consacre un être humain. Ce faisant, **le filtrage automatisé dès les serveurs**

891 LUO Meihan, « China's Content Moderators Are Overworked and Chronically Stressed », sur *Sixthtone.com*, 25 fév. 2022

permet de filtrer une grande quantité de contenus sans ralentir l'accès à un service. Par conséquent, le filtrage par reconnaissance algorithmique ou intelligente est tout à fait adapté pour les applications dont les contenus sont issus d'une forte participation (réseaux sociaux, moteurs de recherche, places de marché...).

Le filtrage automatisé comporte néanmoins deux inconvénients qui en limite l'efficacité. Premier inconvénient : **un filtrage automatisé et homogène** signifie que les failles du filtrage sont elles aussi automatisées et homogènes. L'excès d'homogénéité **peut donc provoquer un contournement beaucoup plus massif qu'un filtrage manuel**, car l'exploitation d'une faille peut être démultipliée par la totalité des utilisateurs. Une faille universelle ouvre la possibilité d'un contournement lui-même universel. Par exemple, après la diffusion d'une vidéo représentant fictivement un suicide sur sa plateforme, TikTok a décidé depuis septembre 2021 de filtrer l'accès de ses utilisateurs aux contenus qui portent certains mots-clés relatifs au suicide, à la mort ou à l'automutilation⁸⁹². À cette fin, les utilisateurs qui accèdent à de tels contenus sont redirigés vers la page d'une association caritative de soutien aux personnes en danger⁸⁹³. Ce filtrage a néanmoins pour effet de priver les utilisateurs en détresse psychologique de pouvoir échanger leurs expériences et témoignages avec les autres utilisateurs, et les psychologues de pouvoir faire connaître des méthodes thérapeutiques. Cette censure a conduit nombre d'internautes à contourner le filtrage en employant des mots non-censurés tels que « unalive », « d3pressi0n »⁸⁹⁴ ... Ainsi, les hashtags #unalivemeplease, #unaliving et #unaliveawareness cumulaient plus de 18 millions de vues en mai 2022.

Deuxième inconvénient du filtrage automatisé : l'application de la règle est si intégrée qu'elle n'offre aucune souplesse d'appréciation. Tous les principes, toutes les exceptions et toutes les circonstances pertinentes d'application doivent donc être prévus par la règle énoncée. Cela signifie que les critères du filtrage doivent être très précisément identifiés pour couvrir exactement la R-DATA ciblée parmi tous les contenus analysés. Par exemple, en Chine, de nombreux réseaux sociaux utilisent des IA pour filtrer les vidéos exposant des mouvements sociaux qui contestent le gouvernement central. Cependant, les critères de filtrage ciblent principalement la présence de pancartes sur une vidéo, ou encore les bruits de foule et cris des manifestants. Des internautes chinois ont alors diffusé leurs vidéos dans des circonstances non prévues par l'IA : en remplaçant le son de la vidéo par une musique de dessin-animé, ou filmant un écran de smartphone qui affiche la vidéo d'une manifestation, les utilisateurs ont pu publier des contenus sans que l'IA ne parvienne à reconnaître la représentation de mouvements contestataires⁸⁹⁵. Il est impossible pour l'énonciateur d'une règle de prévoir toutes les circonstances dans lesquelles une R-DATA peut survenir. **Le filtrage automatisé aggrave**

892TAIT Amelia, « Are TikTok Algorithms Changing How People Talk About Suicide? », *Wired*, mai 2022

893Par-là, TikTok combine deux techniques de régulation : le filtrage de l'accès à une R-DATA (en l'espèce, la R-DATA « contenus incitant au suicide ou à l'automutilation ») ; et le détournement de l'accès vers une A-DATA (en l'espèce la A-DATA « contenus d'aide aux personnes en détresse psychologique »), une technique qu'on examinera plus loin

894TAIT A., « Are TikTok Algorithms Changing How People Talk About Suicide? », préc. V. aussi « TikTok users evade safety filters to share suicide and self-harm posts », *The Times*, oct. 2022

895DORNEL Nelly, « Comment les manifestants chinois contournent l'IA des réseaux sociaux », *Huffington Post*, déc. 2022

donc à la fois le risque de sur-filtrage (filtrage de contenus licites ou admis par le régulateur) **et le risque d'un sous-filtrage concomitant** (non-filtrage de contenus illicites ou refusés par le régulateur).

En somme, le filtrage automatisé de contenus est très loin de garantir au régulateur que le résultat de l'application de la règle sera conforme au résultat qu'il aurait espéré voir. Au lieu de voir filtrés les contenus illicites, le régulateur peut assister à un filtrage des contenus licites (par ex. des vidéos représentant des foules bruyantes hors de tout contexte contestataire), tandis que les contenus illicites (vidéos représentant des foules contestataires) pourront massivement contourner le filtrage et se diffuser sur le service en exploitant les failles automatisées du filtrage.

Face à ce risque, le recours à l'IA apporte un très gros avantage par rapport à l'algorithme : l'algorithme est hétérodidacte, en ce sens que sa connaissance dépend exclusivement de ses règles de programmation (toute sortie de l'algorithme est le résultat direct d'une ou plusieurs entrées insérées par le programmeur) ; inversement, l'IA développe une couche de connaissance qui ne dépend pas de son algorithme mais de sa propre expérience, ce qui en fait un programme auto-apprenant (toute sortie de l'IA est le résultat direct de la connaissance empirique acquise par le programme, l'algorithme se limitant à établir le cadre du traitement de l'information par l'IA et ses règles d'apprentissage). Dès lors, au fil de son expérience, l'IA apprend à détecter telle ou telle méthode de contournement régulièrement répétée et s'adaptera en corrigeant la faille exploitée, de façon à filtrer les contenus issus de cette méthode de contournement. Elle s'adaptera aussi aux erreurs qu'elle commet et qu'elle constate (faux-positifs qui la conduisent à filtrer des contenus licites), ce qui fait de **l'IA un outil de filtrage très prometteur qui relativise largement les principaux inconvénients du filtrage automatisé – l'ampleur du contournement, le sur-filtrage et le sous-filtrage.**

On lui voit cependant un défaut tout aussi spectaculaire : auto-apprenante, l'IA développe ses propres critères de filtrage au point que l'être humain n'a plus de contrôle sur le filtrage effectué. En d'autres termes, **la régulation d'internet par intelligence artificielle fait perdre à l'être humain le contrôle sur la régulation d'internet.** La perte de contrôle de l'être humain sur l'application de la règle de droit au profit de l'IA rend le résultat de la règle de droit nécessairement conforme à ce que décide l'IA, mais pas nécessairement conforme au résultat que souhaite l'être humain ayant posé la règle de droit. Or, une règle de droit a précisément pour objectif de provoquer un résultat conforme à ce que recherche l'être humain. Dès lors, en appliquant le résultat qu'elle recherche, l'IA n'est absolument pas gage d'efficacité d'une règle de droit, mais seulement gage d'efficacité de ses propres règles.

En Chine, le recours au filtrage automatisé s'est très étoffé depuis la deuxième moitié des années 2010. Depuis 2016, la CAC oblige les services de diffusion en direct en ligne à instaurer une plateforme dédiée à l'examen des contenus diffusés, et les services accessibles par applications mobiles à se prêter au même examen⁸⁹⁶. La même année puis l'année suivante, sur le fondement de la loi sur la cybersécurité de la République de Chine, elle étend l'obligation

⁸⁹⁶Respectivement : CAC, Dispositions relatives à l'administration des services de diffusion en direct sur internet (互联网直播服务管理规定) du 4 nov. 2016 ; CAC, Dispositions relatives à l'administration des services d'information pour les applications mobiles sur internet (移动互联网应用程序信息服务管理规定) du 28 juin 2016, art. 8 : « les fournisseurs d'applications sont responsables des résultats de la présentation du contenu d'information, ne produisent pas et ne diffusent pas d'informations illégales, et préviennent consciencieusement les informations indésirables et y résistent », ce qui passe notamment par « des mécanismes d'audit du contenu » et « d'inspection quotidienne ».

d'examen des informations aux fournisseurs de moteurs de recherche, aux services fournissant l'accès à des groupes de discussion en ligne et forums, aux services qui autorisent la publication de commentaires en ligne (réseaux sociaux...) et à ceux qui nécessitent une inscription au moyen d'un compte utilisateur (places de marché...) ⁸⁹⁷. Ces réglementations contraignent par ailleurs ces divers fournisseurs à des méthodes d'analyse des données à travers une « *gestion hiérarchique* » basée sur une catégorisation des contenus, des groupes et des comptes publics, et sur le crédit de publication d'un commentateur en ligne ⁸⁹⁸. Une telle organisation doit permettre aux services d'identifier les utilisateurs problématiques pour supprimer promptement les contenus illicites qu'ils produisent, pour les bannir partiellement ou totalement du service, ou encore pour adopter des « *mesures préventives* » qui s'étendent au-delà des utilisateurs problématiques. En s'appuyant sur cette gestion des informations, les services susmentionnés doivent filtrer principalement deux types de données : les données anonymes ; et les contenus illicites.

Doivent d'abord être filtrées les données anonymes : depuis 2015, la CAC mène une politique dite « *volonté au guichet et vrais noms en arrière-boutique* » (*voluntary backstage real name frontstage*, 后台实名前台自愿) qui consiste à s'assurer de l'identité réelle de chaque utilisateur d'un service en ligne ⁸⁹⁹. Légalement, cela se traduit par l'obligation faite aux fournisseurs de services susmentionnés d'authentifier l'identité réelle des utilisateurs de leurs services au moyen de documents prouvant cette identité (carte bancaire, carte d'identité...) ⁹⁰⁰. La quasi-totalité des fournisseurs de services en ligne chinois possèdent ainsi les informations sur l'identité réelle de chaque utilisateur grâce au téléchargement de pièces d'identité. Doivent ensuite être filtrées les contenus illicites : en 2022, la CAC propose de modifier les dispositions de 2017 relatives aux commentaires sur internet, lesquelles prévoyaient le filtrage de commentaires sous des actualités ou provenant de comptes inscrits sur liste noire. La modification apportée lève ces

⁸⁹⁷Respectivement : CAC, Dispositions relatives à l'administration des services de recherche d'informations sur internet (互联网信息搜索服务管理规定) du 25 juin 2016, art. 6 ; CAC, Dispositions relatives à l'administration des services d'information des groupes sur internet (互联网群组信息服务管理规定) du 7 sept. 2017, art. 5 ; CAC, Dispositions relatives à l'administration des services pour les forums et communautés sur internet (互联网论坛社区服务管理规定) du 25 août 2017, art. 5 ; CAC, Dispositions relatives à l'administration des services de commentaire sur internet (互联网跟帖评论服务管理规定) du 25 août 2017, art. 5 (devenu art. 6 depuis la révision de 2019) ; et CAC, Dispositions relatives à l'administration des informations sur les comptes publics des utilisateurs d'internet (互联网用户公众账号信息服务管理规定) du 7 sept. 2017

⁸⁹⁸Art. 7 des dispositions relatives à l'administration des services de diffusion en direct sur internet (catégorisation des contenus), à l'administration des services de diffusion en direct sur internet relatives à l'administration des informations sur les comptes publics des utilisateurs d'internet (catégorisation des comptes), à l'administration des services d'information des groupes sur internet (catégorisation des groupes), et art. 9 des dispositions relatives à l'administration des services de commentaire sur internet (catégorisation selon le crédit de publication)

⁸⁹⁹Page « *volonté au guichet et vrais noms en arrière-boutique* (后台实名前台自愿) » de l'encyclopédie chinoise en ligne Baidu Baike [<https://baike.baidu.com/item/后台实名前台自愿/16591011>]. Cette politique est annoncée par la CAC lors d'une conférence de presse du 13 janvier 2015.

⁹⁰⁰Dispositions relatives à l'administration des services de diffusion en direct sur internet, art. 12 ; articles 6 des dispositions relatives à l'administration des services d'information pour les applications mobiles sur internet, relatives à l'administration des services d'information des groupes sur internet et relatives à l'administration des informations sur les comptes publics des utilisateurs d'internet ; dispositions relatives à l'administration des services pour les forums et communautés sur internet, art. 8 ; dispositions relatives à l'administration des services de commentaire sur internet, art. 5(1)

conditions pour généraliser la censure préventive de l'ensemble des commentaires, obligeant les prestataires à filtrer tout commentaire en ligne avant publication, qu'il relève ou non d'un sujet d'actualité, d'un utilisateur suspect ou d'une discussion animée⁹⁰¹. Une telle généralisation ne permet plus de recourir exclusivement à une modération humaine *a priori* pour filtrer les contenus, et oblige alors les fournisseurs de services de commentaires en ligne à employer un filtrage par reconnaissance algorithmique ou intelligente.

Au niveau de l'Union Européenne (UE), le recours au filtrage automatisé dès les serveurs a été amorcé vers la fin des années 2010, sur le terrain des œuvres protégées par un droit d'auteur/voisin. À travers la directive « droit d'auteur » de 2019 (« directive Damun »), le droit de l'UE a d'abord inclus de nouveaux acteurs dans la protection des droits d'auteur : les « fournisseurs de services de partage de contenus en ligne », *i.e.* toute plateforme (réseaux sociaux, plateformes de partage de fichiers, moteurs de recherche...) qui tire consciemment profit ou qui espère tirer profit des violations de droits d'auteur diffusées sur son service⁹⁰². En profitant de ces diffusions, ou en ne les empêchant pas alors qu'elle connaît ou contrôle les contenus téléchargés⁹⁰³, la plateforme accomplit un acte de « communication au public » d'une œuvre protégée. Or, un tel acte relève du droit exclusif du titulaire du droit d'auteur sur l'œuvre, ce qui oblige la plateforme à obtenir l'autorisation préalable du titulaire avant de pratiquer une communication au public. Pour cette raison, l'art. 17 de la directive Damun tient les fournisseurs de services de partage de contenus en ligne pour responsables de tout contenu violant un droit d'auteur si ces fournisseurs n'ont pas déployé les « *meilleurs efforts* » pour (i) obtenir une autorisation préalable du titulaire du droit d'auteur, (ii) garantir l'indisponibilité à long terme des contenus litigieux *et* (iii) empêcher le téléversement (transfert de fichiers du client vers le serveur, ou *upload*) des contenus litigieux ou les supprimer une fois signalés par les titulaires.

De nombreux commentateurs avaient souligné que, dans les faits, il est impossible au fournisseur d'obtenir une autorisation préalable des ayants droit pertinents avant la diffusion de chaque contenu violant un droit d'auteur diffusé sur son service. Par conséquent, si la responsabilité du fournisseur est conditionnée par l'obtention d'une autorisation préalable de diffusion de chaque contenu violant un droit d'auteur diffusé sur son service, le fournisseur ne peut échapper avec certitude à la mise en cause de sa responsabilité qu'en censurant ces contenus avant même leur diffusion, donc en filtrant ces contenus⁹⁰⁴. L'interprétation faite de

901CAC, Avis sur les dispositions relatives à l'administration des services de commentaire sur internet (projet de révision publiquement soumis aux commentaires des internautes) (互联网跟帖评论服务管理规定 (修订草案征求意见稿)) du 17 juin 2022

902Directive 2019/790 du 17 avr. 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique, art. 2, (6) : le fournisseur de services de partage de contenus en ligne est défini comme le fournisseur de services en ligne « dont l'objectif ou l'un des objectifs principaux est de stocker et de donner au public l'accès à une quantité importante d'œuvres protégées par le droit d'auteur ou d'autres objets protégés qui ont été téléversés [comprendre "téléchargés"] par ses utilisateurs, qu'il organise et promeut à des fins lucratives »

903CJUE, *Pologne c. Parlement européen et Conseil de l'Union européenne*, 26 avr. 2022, aff. C-401/19, §27. La Cour précise par la même occasion qu'un hébergeur peut par ailleurs avoir la qualité de fournisseur de services de partage de contenus en ligne, auquel cas cet hébergeur est soumis aux obligations de la directive (§28).

904Par ex., REES Marc, « Directive Droit d'auteur : notre schéma pour comprendre l'article 13 », *NextInpact*, mars 2019 : « le texte ne parle pas explicitement de filtrage, mais [la plateforme] doit

la directive Damun par la CJUE en 2022 clarifie la question. Après avoir rappelé que cette censure ne couvre pas les exceptions au droit d'auteur (citation, critique, revue, caricature, parodie et pastiche), elle juge qu'instaurer une censure préventive des contenus librement appréciée par les fournisseurs de services serait contraire à la liberté d'expression et d'information ainsi qu'à l'interdiction faite aux États membres de soumettre les hébergeurs et opérateurs à une obligation de surveillance générale des contenus⁹⁰⁵. Cependant, elle admet l'obligation faite par la directive aux plateformes de filtrer certains contenus spécifiques, par exemple : en empêchant la réapparition d'un contenu déjà signalé pour avoir violé un droit d'auteur ; ou encore, en censurant préventivement les contenus issus d'un utilisateur identifié et notifié par les ayant-droit comme auteur régulier de contenus violant un droit d'auteur. Sous ces modalités, la Cour de justice espère que le système de filtrage automatisé évitera de censurer des contenus licites – une telle censure étant par elle-même contraire à la liberté d'expression⁹⁰⁶.

C) Le filtrage de contenus dès les serveurs

Le filtrage de contenus dès le serveur consiste à empêcher, depuis un serveur, la production de contenus avant même leur hébergement. Le **filtrage de contenus** présente le premier avantage d'empêcher la production même d'un contenu, *i.e.* **d'intervenir avant toute amplification des échelles de diffusion et de production d'un contenu**. À titre de comparaison, bien que le masquage *ex ante* intervienne avant l'amplification de l'échelle de diffusion, il n'intervient pas avant l'amplification de l'échelle de production. Le **deuxième avantage du filtrage de contenus** tient dans le fait qu'il cible des contenus. Contrairement au bannissement, le filtrage de contenus ne repose pas sur des données authentifiant les utilisateurs mais sur des données de contenu, et **ne requiert donc pas d'identifier des utilisateurs suspects pour leur appliquer des mesures de restriction**. Inversement, bien que le bannissement total intervienne avant l'échelle de diffusion et de production en privant un utilisateur du pouvoir de produire des contenus sur le service dont il est banni, un tel bannissement requiert d'identifier préalablement l'utilisateur suspect qui se verra banni.

Le **filtrage de contenus** s'accompagne néanmoins de deux inconvénients. D'abord, nécessairement automatisé, il doit prévoir tous les principes, exceptions et circonstances d'application de la règle avant la survenance d'un cas concret, ce qui **aggrave le risque de sur-filtrage**. Ensuite, du fait de son automatisation, il automatise des failles exploitables par tous les utilisateurs, ce qui **facilite le contournement du système de filtrage**.

Cet inconvénient de faciliter le contournement est corrigé lorsque le filtrage de contenus est initié par les utilisateurs. On voit deux avantages au **filtrage de contenus initié par l'utilisateur**. D'une part, la liste de données de contenu filtrés (texte, image, son, vidéo) est bien plus imprévisible si chaque utilisateur établit sa propre liste, ce qui rend le filtrage **nettement**

*suivre "les standards de haut niveau issus des règles de diligence professionnelle". Le filtrage fait nécessairement partie de ces réponses techniques. ». V. aussi TREPPOZ Edouard, « Premiers regards sur la directive droit d'auteur dans le marché numérique », JCP A, juill. 2019. 1343 ; BENSAMOUN Alexandra, « Filtrage des contenus par les plateformes contributives et liberté d'expression », *Légipresse*, sept. 2021, p. 399s.*

905CJUE, *Pologne c. Parlement européen et Conseil de l'Union européenne*, 2022, préc., §37 et 90.

V. aussi le commentaire de SIRINELLI Pierre « La portée des solutions proposées par l'article 17 de la directive (UE) 2019/790 du 17 avril 2019 au lendemain de sa transposition en droit français et de l'arrêt du 26 avril 2022 de la Cour de justice de l'Union européenne », *Légipresse*, n°67, 2022, p. 149s.

⁹⁰⁶ *Ibid.*, §85 à 89

plus difficile à contourner par comparaison avec une liste unique valant pour tous les utilisateurs de l'application. Notons cependant que le filtrage de contenus initié par les utilisateurs est plus facile à contourner que le masquage de contenus *ex ante* initié par les utilisateurs. En effet, dans le cas du filtrage, il n'est pas possible de dissimuler à un utilisateur que son contenu a été filtré, car c'est sa tentative même de production qui est empêchée. Inversement, le masquage admet que soit hébergé le contenu illicite produit mais en empêche l'accès aux autres utilisateurs, ce qui permet de maintenir l'auteur du contenu masqué dans l'ignorance du masquage opéré. La source de masquage (utilisateur masqueur) est dans ce cas plus imprévisible que peut l'être la source de filtrage (utilisateur filtreur). D'autre part, les utilisateurs sont la catégorie d'acteurs la mieux positionnée pour identifier les contenus contraires à leur volonté (indésirables) et celle qui contribue le plus directement à l'échelle de diffusion d'une donnée. Remettre de tels outils de filtrage aux utilisateurs permet donc de **réduire directement l'échelle de production et de diffusion des contenus indésirables**. Ces avantages – qu'on retrouve aussi avec le bannissement et le masquage *ex ante* (limité à réduire l'échelle de diffusion) initiés par l'utilisateur – font de ces diverses techniques initiées par les utilisateurs des techniques de régulation très intéressantes pour lutter contre les stockages indésirables de données⁹⁰⁷.

Le **filtrage de contenus initié par l'utilisateur** présente cependant deux inconvénients. D'une part, les utilisateurs n'initieront le filtrage qu'à l'encontre de contenus contraires à leur volonté, ce qui en fait une **technique inadaptée contre des données illicites auxquelles les utilisateurs accèdent intentionnellement**. D'autre part, si le pouvoir de filtrage remis à chaque utilisateur permet d'empêcher un autre utilisateur de *publier* des contenus, n'importe quel utilisateur peut exercer ce pouvoir pour empêcher n'importe quel autre utilisateur de produire des contenus sur les espaces publics de l'application. On retrouve donc la limite du bannissement initié par l'utilisateur – lorsque le bannissement est total, il fait courir le risque que des jeux de pouvoir s'emparent de l'application, par lesquels des utilisateurs totalement bannis voient leur liberté d'utiliser l'application violée voire anéantie par des utilisateurs bannis. Afin d'éviter ce type de stratégies, **le filtrage initié par un utilisateur doit être strictement limité** – en limitant les contenus filtrables aux seuls contenus privés (*i.e.* en principe non accessibles à un public comme les messages privés), ou encore en limitant le nombre d'utilisateurs capables de filtrer des contenus publics tiers aux seuls utilisateurs reconnus victimes par un tribunal et contre les seuls contenus de son agresseur (ce serait toutefois faire de la victime un organe d'application de la décision de justice qui la concerne, ce qui ne nous semble pas souhaitable). De la même manière que le bannissement initié par l'utilisateur peut difficilement s'étendre au-delà du bannissement partiel, le filtrage de contenus initié par l'utilisateur peut difficilement s'étendre au-delà des espaces privés (compte utilisateur, messagerie privée...).

Par opposition, le **filtrage de contenus initié par l'application** porte les avantages et inconvénients contraires à ceux étudiés. Il a pour premier avantage de pouvoir **couvrir tous les contenus illicites**, qu'ils soient ou non indésirables pour l'utilisateur. Il a pour deuxième avantage de pouvoir **s'exercer sur tous les espaces logiques d'une application** – publics comme privés – sans provoquer de jeux de pouvoir entre utilisateurs (stratégies d'exclusion d'utilisateurs par d'autres utilisateurs). Dans l'Union européenne, il est toutefois fait interdiction à

⁹⁰⁷ La maîtrise des stockages indésirables (ou « stockages accidentels ») est un avantage décisif pour réguler efficacement le réseau internet, comme on le verra plus loin

l'application de filtrer les messages privés, généralement par respect du secret des correspondances privées et de la liberté d'expression⁹⁰⁸.

Le filtrage de contenus initié par l'application a pour premier inconvénient de **faciliter le contournement** en instaurant une unique source de filtrage – le système de filtrage de l'application. Pour contourner le filtrage initié par l'application, il suffit ainsi de produire un contenu méconnu par une seule liste de contenus censurés : celle établie par l'application. Deuxièmement, l'échelle de diffusion d'un contenu n'est pas constituée par l'application mais par le nombre de ses utilisateurs qui accèdent à ce contenu sans l'avoir produit. En filtrant mutuellement leurs contenus, les utilisateurs peuvent donc réduire directement l'échelle de diffusion et de production d'un contenu, tandis que le filtrage de contenus initié par l'application n'agit directement que sur l'échelle de production du contenu. Pour le dire autrement, un contenu qui contourne le filtrage initié par l'application peut être vastement consulté et acquérir une grande échelle de diffusion si aucun utilisateur ne le filtre ; inversement, un contenu qui contourne le filtrage initié par un seul utilisateur ne contournera pas de ce fait les filtrages initiés par d'autres utilisateurs, ce qui limite doublement la production et la diffusion de ce contenu. Dès lors, par rapport au filtrage initié par l'utilisateur, **le filtrage initié par l'application a pour inconvénient d'aggraver le risque de diffusion d'un contenu illicite ou indésirable en cas de contournement.**

Contrairement au filtrage de contenus initié par l'utilisateur qui est nécessairement automatisé (donc aggravateur du risque de sur-filtrage), le filtrage de contenus initié par l'application peut être manuel – dans le cadre d'une modération humaine *a priori* – ou automatisé. Si le filtrage initié par l'application est manuel, il hérite des avantages (réduction du risque de sur-filtrage, difficulté relative de contournement) et inconvénients (impossibilité de filtrer un gros volume de contenus, hétérogénéité voire incohérences de l'application de la règle de filtrage) de tout filtrage manuel. S'il est automatisé, il hérite des avantages (homogénéité de l'application de la règle de filtrage, possibilité de filtrer un gros volume de contenus) et inconvénients (facilité de contournement par l'automatisation des failles exploitables et aggravation du risque de sur-filtrage) de tout filtrage automatisé.

Qu'il soit manuel ou automatisé, initié par l'utilisateur ou l'application, le filtrage de contenus peut cibler les quatre types de données de contenu connus à ce jour : texte, image, son et vidéo. La technique adaptée dépend de la provenance de la R-DATA. Si la R-DATA provient d'un format texte, le filtrage par reconnaissance de caractères sera adapté. Le filtrage par reconnaissance de caractères consiste, dès le serveur, à empêcher la production de contenus portant certains caractères ou suites de caractères (mots, expressions, émojis, signes de ponctuation...). On en a déjà croisé plusieurs exemples, comme la censure par mots-clés haineux pratiquée par

⁹⁰⁸ Cette interdiction a encore été rappelée récemment par le Règlement 2021/1232 du 14 juil. 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne. Ce règlement autorise les entreprises volontaires à scanner les messages privés de mineurs pour détecter et signaler aux autorités compétentes de potentiels abus sexuels, mais précise que le scan est seulement autorisé à détecter des messages suspects sans pouvoir en empêcher la production (considérant 16 : « *ces technologies [de scan] ne devraient pas être utilisées pour le filtrage et l'examen systématiques du texte dans les communications, excepté s'il s'agit seulement de détecter des schémas qui indiquent d'éventuels motifs concrets de soupçons d'abus sexuels commis contre des enfants en ligne, et elles ne devraient pas être capables de déduire la substance du contenu des communications* »).

le forum JVC, ou la censure par mots-clés suicidaires pratiquée par TikTok – toutes deux contournées par de nombreux utilisateurs. Dans ces cas, le filtrage est initié par l'application.

Si la R-DATA provient d'un format image, le filtrage par reconnaissance d'images sera adapté. Par exemple, en Chine, les utilisateurs sont habitués à contourner le filtrage par reconnaissance de caractères en publiant des jeux de mots, des émojis ou encore des textes sous format d'images⁹⁰⁹ (non détectés par un filtrage de caractères, qui cible les formats texte). Pour empêcher ce dernier mode de contournement, les algorithmes des principaux réseaux sociaux chinois ont été mis à jour pour pouvoir scanner les images et identifier les textes qu'elles contiennent. En réponse, des utilisateurs ont contourné cette mise à jour en faisant pivoter les textes mis en image pour empêcher la reconnaissance d'un texte par le scan algorithmique (l'inversion des caractères est très lisible pour l'être humain dans la typographie chinoise)⁹¹⁰.

Enfin, si la R-DATA provient d'un format vidéo et/ou audio, le filtrage par reconnaissance vidéo et/ou audio sera adapté. Par exemple, pour lutter contre la diffusion de contenus violant les droits d'auteur, YouTube s'appuie sur une base de données de contenus, composée par les extraits audio et vidéo soumis régulièrement à YouTube par les ayants droit : « *lorsque Content ID [algorithme d'analyse des contenus de YouTube] trouve une correspondance, il peut (...) : bloquer l'affichage d'une vidéo / monétiser la vidéo en y diffusant des publicités et en partageant parfois les revenus avec l'auteur de la mise en ligne / suivre les statiques d'audience de la vidéo* »⁹¹¹. On pense que, pour appliquer le filtrage des violations de droits d'auteur exigé par la directive européenne Damun, YouTube s'appuiera sur la même base de données.

⁹⁰⁹ En 2009, les utilisateurs chinois qualifiaient les censeurs d'internet de « crabes de rivière » (河蟹, *Hexie*, un homophone de « harmonie ») et les opposants à la censure de « lamas boueux » (草泥马, *Cao Ni Ma*, un homophone de « fils de pute ») : NIVELLE Pascale, « "Caonima", le clip qui fait la nique à Pékin », *Libération*, 16 mars 2009. En 2018, pour continuer à échanger sur le sujet des agressions contre les femmes et contourner la censure des mots clés « Me Too » (#我也是, #米兔), les utilisateurs emploient les émoticônes d'un bol de riz (Mi) et d'un lapin (Tu) ou encore le hashtag #RiceBunny : BAO Han, « "Rice Bunnies" – #MeToo in China: A hashtag movement and women's empowerment through social media », *Conference: Proceedings of EVA London*, juil. 2019. À la fin des années 2010, les utilisateurs chinois avaient développé un véritable langage pour contourner la censure : les lettres « wh » pour parler de Wuhan (premier centre de l'épidémie de Covid19 en Chine), « hb » pour parler de Hubei, « zf » pour désigner le gouvernement, « gc » pour désigner la police, des images de pandas pour identifier le Bureau de la sécurité intérieure, le « ministère de la Vérité » (tiré de l'œuvre 1984 de George Orwell) pour parler du Département de la propagande du Parti communiste, ou encore « nouilles pho vietnamiennes » (quasi-homophone de « passer de l'autre côté du mur ») pour se référer aux VPN : « Des nouilles pho et des pandas. Comment les internautes en Chine inventent un langage pour contourner la censure liée au COVID-19 », *Amnesty International*, 6 mars 2020

⁹¹⁰ ZHANG Karen, « The promises and pitfalls of digital activism: Fighting for #MeToo under the Great Firewall of China » [en ligne], *ANU Undergraduate Research Journal*, vol. 11, n° 1, avr. 2021

⁹¹¹ « How Content ID works », sur *Support.google.com* [consulté le 29 mars 2023]

Sous-Partie 2. Étude de l'efficacité régulatrice sur internet

Plusieurs techniques de restriction ont jusqu'à présent été analysées au regard de leurs avantages et inconvénients. La connaissance de ces avantages et inconvénients permettent de savoir dans quels cas une technique de restriction est adaptée ou inadaptée. Cependant, ils ne donnent pas la possibilité de mesurer l'efficacité de l'action régulatrice lorsqu'elle intervient. Cette Sous-Partie 2 a vocation à réfléchir aux moyens d'évaluer ladite efficacité.

Elle sera aussi et surtout l'occasion d'examiner les techniques d'augmentation de l'accès à une donnée - et donc les A-DATA. *A priori*, les techniques d'augmentation de l'accès peuvent sembler à la fois plus inoffensives et moins efficaces que les techniques de restriction, parce qu'elles n'empêchent pas directement l'accès à une R-DATA. On verra que les techniques de régulation par augmentation de l'accès peuvent se révéler non seulement plus efficaces sur l'échelle de diffusion d'une donnée (y compris d'une R-DATA) que les techniques de restrictions, mais aussi plus attentatoires aux libertés dans plusieurs situations : la surexposition de données par des algorithmes prive l'utilisateur de sa liberté de consommer les contenus qu'il souhaite (donc de sa liberté de communiquer en ligne⁹¹²), et peut valoriser des contenus violents, haineux voire pornographiques contraires à l'intérêt ou à la volonté de l'utilisateur ; la redirection du trafic peut priver l'utilisateur de sa liberté d'accéder au service qui fait l'objet de cette redirection ; la réutilisabilité des données peut conférer au propriétaire de ces données un pouvoir sur toutes les personnes et tous les programmes qui réutilisent ces données, devenant ainsi dépendants économiquement voire personnellement ou socialement desdites données etc.

On examinera donc en premier lieu certaines méthodes pour évaluer la mesure dans laquelle une technique de régulation peut agir sur le réseau internet. On illustrera ce travail à travers la techniques de la centralisation, qui nous permettra d'en déduire l'état général de la centralisation d'internet en 2022 (**Chapitre 1**). Cependant, cette évaluation de la *mesure d'action* de la technique de centralisation sur le réseau internet ne permet pas d'en évaluer l'*efficacité*, c'est-à-dire la mesure dans laquelle cette technique réduit l'échelle de diffusion d'une R-DATA ou amplifie celle d'une A-DATA. C'est pourquoi, en second lieu, après avoir décrit sept techniques de régulation par augmentation, on s'attachera à évaluer l'efficacité des techniques de régulation dans telle ou telle circonstances, et on proposera une méthode qui se veut systématique pour améliorer l'efficacité des techniques de régulation. On constatera à cette occasion que les techniques de restriction et d'augmentation sont souvent complémentaires (**Chapitre 2**).

⁹¹² Bien que le Conseil constitutionnel ait limité en 2009 la liberté d'accès « aux services de communication au public en ligne » au seul droit pour une personne d'être « connectée » à internet (CC, *Hadopi 1*, 10 juin 2009, n° 2009-580 DC et commentaire de la décision), il a en 2017 étendu cette liberté au droit pour une personne d'utiliser internet pour « chercher des informations » sans devoir être inquiété par la loi (CC, *M. David P.*, 2017, n° 2017-682 QPC et commentaire de la décision). N'est donc plus seulement consacrée la liberté d'accès matériel à internet (droit d'être connecté aux infrastructures réseau) mais la liberté d'accès logiciel à internet (droit de « naviguer » sur internet en y cherchant des informations). Cette dernière liberté ne protège pas, à ce jour, les internautes contre les biais algorithmiques qui nuisent à leur libre consultation des contenus, mais c'est une avancée dans cette direction - avancée par ailleurs complétée par le Digital Service Act européen de 2022 qui oblige les très grandes plateformes à fournir à leurs utilisateurs les moyens de désactiver les algorithmes de suggestion.

Chapitre 1. La technique de la centralisation du réseau

La centralisation d'internet ne s'évalue pas sur un seul terrain. Elle concerne de nombreuses fractions du réseau internet - centralisation des câbles terrestres et sous-marins, des satellites, de l'acheminement par les routeurs, des noms de domaine, des applications... Par ailleurs, pour une même fraction d'internet, on rapportera plusieurs types de centralisations différentes - centralisation du fonctionnement de cette fraction, de sa gestion, de sa conception, des connexions que suscite cette fraction dans le monde etc.

On étudiera d'abord trois fractions du réseau qui semblent de moins en moins centralisées depuis l'apparition d'internet : la transmission de données par câbles sous-marins ; la transmission de données par le routage ; et le stockage des noms de domaine. On verra néanmoins que ce mouvement de décentralisation doit être largement relativisé. La Russie centralise de plus en plus chacune de ces trois fractions ; la Chine n'a que très relativement décentralisé son réseau d'acheminement, et la France conserve un réseau d'acheminement lui aussi fortement centralisé ; la gestion des câbles sous-marins est certes moins centralisée que dans le passé, mais une tendance récente introduit une centralisation accrue de cette gestion par les « géants » d'internet ; et le système des noms de domaine, bien que de plus en plus décentralisé par son fonctionnement, maintient sa gestion très centralisée par l'Icann. On observera alors que ces centralisations survivantes menacent la sécurité du réseau (Section 1).

Ensuite, on examinera la centralisation des usages en ligne à travers les applications. À ce titre, on constate que les applications sont de plus en plus centralisées mondialement depuis les années 1990, tant en ce qui concerne leur gestion que leur fonctionnement et le nombre de connexions à ces applications. On remarquera que cette centralisation aggrave considérablement les conditions d'égale concurrence, lesquelles ont de moins en moins de sens dans le secteur des usages en ligne (Section 2).

Section 1. La centralisation de la transmission de données et des noms de domaine

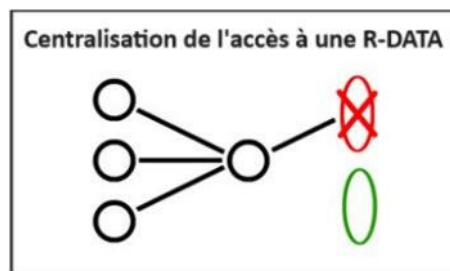
Sera évaluée la centralisation de la transmission de données en Chine, en France, en Russie, au Royaume-Uni et en Corée du Nord (Paragraphe 1) puis, au stade du stockage de données, la centralisation des noms de domaine (Paragraphe 2).

Paragraphe 1 – La centralisation de la transmission de données

On commencera par étudier la centralisation du transport sous-marin (A). On recherchera ensuite les métriques permettant de mesurer la centralisation d'un réseau (B), avant de comparer le degré de centralisation des différents réseaux d'acheminement (C) et d'isoler l'examen du réseau d'acheminement le plus centralisé au monde - la Corée du Nord (D).

A) La centralisation du transport sous-marin

La dernière technique de restriction qu'on étudie est celle de la centralisation. On appelle « centralisation de l'accès à la R-DATA » la technique qui consiste à faire d'un nœud destinataire le seul qui permette l'accès à la R-DATA par un grand nombre de nœuds émetteurs. Au niveau de la transmission (transport et acheminement), cette technique est généralement employée pour empêcher l'accès à des données étrangères, en créant un goulot d'étranglement enfermant l'accès à la R-DATA « données étrangères ». Lorsque la



centralisation est effectuée dès l'acheminement, le routeur occupe la position du nœud destinataire central.

En France, aux États-Unis et au Royaume-Uni, nous n'avons identifié que peu de traces d'une centralisation *étatique* dès la transmission. Il y existe certes une centralisation sur le marché des opérateurs, mais cette centralisation est surtout d'initiative privée. Ainsi, dans chacun des trois pays, seuls quatre opérateurs de téléphonie mobile représentent plus de 90% des parts de marché ⁹¹³. Or, cette centralisation sur le marché résulte des comportements d'acteurs privés bien plus que des comportements d'acteurs publics. En déployant très tôt de vastes lignes téléphoniques et en rachetant certains réseaux concurrents, les principaux opérateurs privés ont acquis des infrastructures essentielles (réseaux dorsaux) à toute connexion internet et donc un avantage concurrentiel favorisant leur position dominante sur le marché⁹¹⁴. Le caractère privé ou étatique de la centralisation indique seulement l'acteur qui pratique la centralisation (acteurs privés ou État), mais n'indique pas l'intensité de la centralisation. Cela nous amène à comparer les centralisations d'initiative étatique russe, chinoise et iranienne avec les centralisations d'initiative privée française, britannique et américaine, dans le but de répondre à la question : lesquelles de ces centralisations sont les plus intenses ?

Pour mener une comparaison entre ces divers pays, on étudie la centralisation du réseau à une même échelle – celle d'un réseau national de transmission. Par « réseau national de transmission », on entend les équipements de transmission (routeurs, câbles sous-marins, antennes-relais...) et les réseaux de transmission (AS, réseaux sous-marins, réseaux aériens...) présents sur le territoire national d'un pays. **On évalue la centralisation d'un réseau national de transmission à partir de la diversité des voies d'accès fournies par ce réseau.** Par « voie d'accès en ligne », ou encore « voies / canaux de communication », on désigne les moyens physiques et logiques qui permettent la communication entre deux machines (câbles sous-marins, routeurs, adresses IP...). Lorsque ces moyens permettent la communication entre deux machines présentes sur le territoire, on parlera de « voies nationales d'accès » du réseau national. Lorsqu'ils permettent la communication entre une machine présente sur le territoire et une machine présente sur un territoire étranger, on parlera de « voies internationales d'accès » du réseau national. On évaluera dès lors la diversité des voies d'accès d'un réseau national sur deux terrains : la diversité des voies nationales d'accès pour les échanges au sein du réseau national ; et la diversité des voies internationales d'accès pour les échanges entre le réseau national et les réseaux étrangers.

D'un côté, une centralisation des voies nationales d'accès indique que les équipements de transmission présents sur le territoire national limitent les voies de communication entre deux machines présentes sur ce même territoire. Plus est forte la centralisation des voies nationales, plus sont limitées les voies de communication au sein du réseau national, plus les équipements de transmission placent le trafic national dans un goulot d'étranglement. On voit plusieurs critères qui révèlent la diversité des voies nationales d'accès : le nombre d'opérateurs différents qui gèrent les principaux équipements ; le nombre d'équipements de transmission (routeurs, câbles sous-marins, antennes...) ou le nombre de réseaux de transmission (réseaux sous-marins, réseaux aériens,

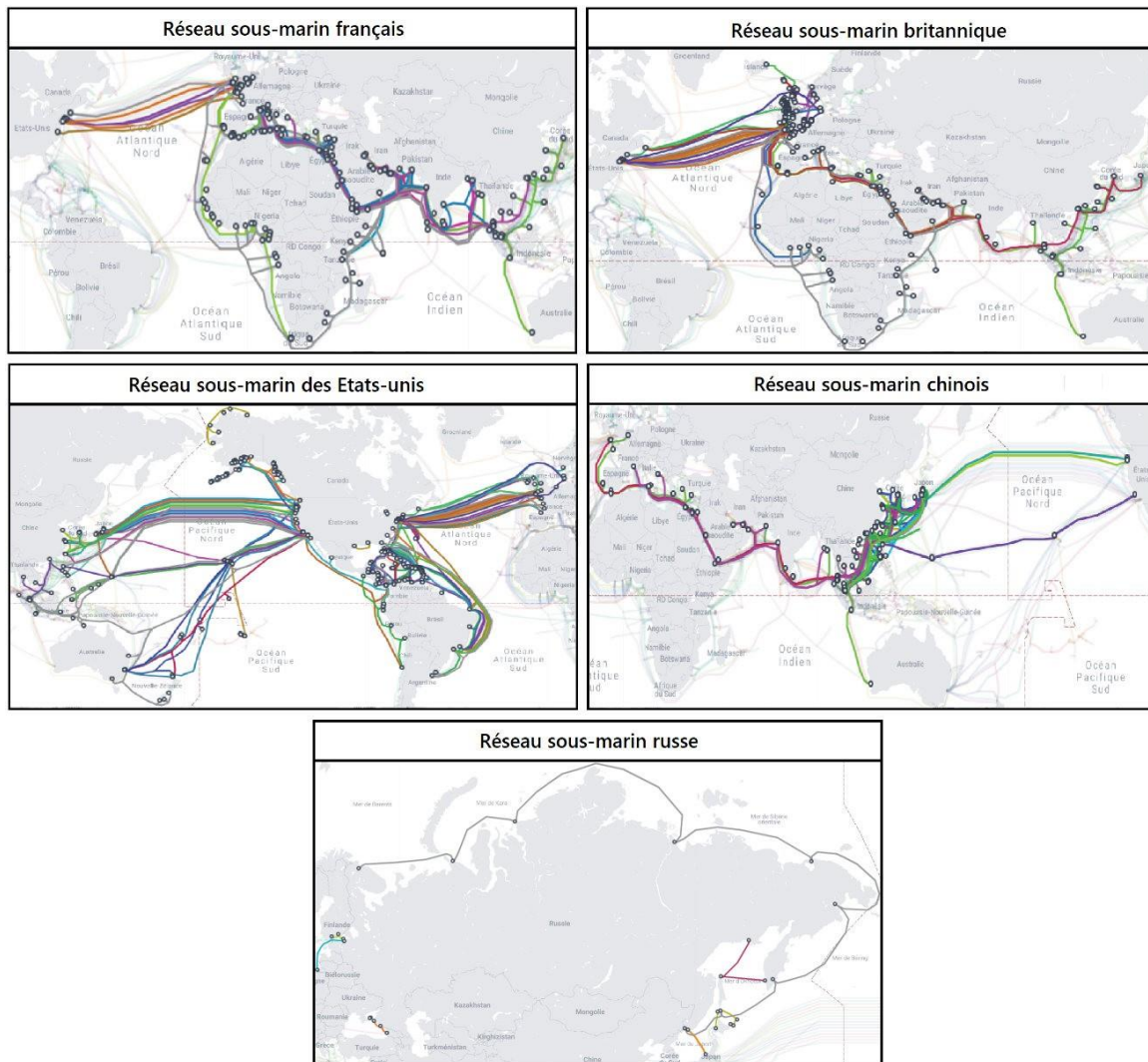
913Orange, SFR, Bouygues et Free en France ; Verizon, AT&T, T-Mobile et Sprint aux États-Unis ; TalkTalk, BT, O2 (Virgin Media) et Sky au Royaume-Uni

914PÉNARD Thierry, « L'accès au marché dans les industries de réseau », *Revue internationale de droit économique*, t. XVI, Association internationale de droit économique, 2002, p. 293-312

réseaux de routeurs dits « *autonomous systems* »...) nécessaire pour connecter au réseau national l'essentiel des machines présentes sur le territoire ; le nombre d'équipements ou de réseaux de transmission qui transmettent l'essentiel du trafic national ou qui sont les mieux desservies par les routes du réseau etc.

De l'autre côté, une centralisation des voies internationales d'accès indique que les équipements de transmission présents sur le territoire national limitent les voies de communication entre une machine présente sur ce même territoire et une machine présente sur un territoire étranger – ce qui inclut à la fois les accès à un réseau étranger depuis le réseau national (« connexions sortantes », *outbound connections*) et les accès au réseau national depuis un réseau étranger (« connexions entrantes », *inbound connections*). Plus est forte la centralisation des voies internationales, plus sont limitées les voies de communication entre le réseau national et les réseaux étrangers, plus les équipements de transmission placent les connexions entrantes et sortantes dans un goulot d'étranglement. Pour les accès internationaux, la diversité des voies d'accès est révélée par d'autres critères tels que : le nombre d'opérateurs différents qui gèrent les principaux équipements transmettant des données à des réseaux étrangers ; le nombre d'équipements ou de réseaux de transmission connectés à des réseaux étrangers ; le nombre de réseaux étrangers connectés au réseau national etc.

À travers la diversité des voies nationales et internationales d'accès dans un réseau national, on peut ainsi estimer combien sont centralisés les réseaux de transport sous-marin russe, chinois, français, britannique et américain les uns par rapport aux autres. Pour réaliser cette estimation, on s'est servi de la base de données Submarine Cable Map (submarinecablemap.com) qui répertorie les données relatives au trajet, aux stations, aux propriétaires et aux fournisseurs des câbles sous-marins, et sur la base de données Submarine Networks (submarinenetworks.com) qui décrit l'histoire et les caractéristiques des installations et des propriétaires des câbles sous-marins. Extraites de Submarine Cable Map, les cartes suivantes dessinent les réseaux sous-marins nationaux ici comparés.



Chaque réseau sous-marin national est constitué par les câbles rattachés au territoire national concerné. Ces cartes appellent une première observation : la singularité du réseau sous-marin russe par rapport aux quatre autres. D'abord, le réseau sous-marin russe est connecté à très peu de territoires étrangers mais surtout, il comporte un câble immense de 12 650km qui relie exclusivement des stations du territoire russe. Ce câble baptisé « Polar Express » est le fruit d'un projet du gouvernement fédéral russe débuté en 2021 et censé s'achever en 2026, pour lequel l'État a investi 889 millions de dollars⁹¹⁵. Le but du projet est d'assurer l'autosuffisance du réseau russe dans le cas d'une panne internationale ou d'une menace provenant du réseau extérieur : même si la Fédération bloquait, filtrait voire coupait tout accès internet à un réseau étranger, le Polar Express pourrait à lui seul continuer de transporter tout le trafic sous-marin national⁹¹⁶. Le propriétaire et gestionnaire du Polar Express est l'État fédéral à travers le ministère des Transports, l'Agence fédérale pour le transport maritime et

915STOLYAROV Gleb, « Russia starts operation to lay undersea fibre optic cable through Arctic », *Reuters*, 6 août 2021

916Cette autosuffisance sous-marine ne signifie pas en elle-même la possibilité pour la Russie de s'isoler du réseau international, mais seulement la possibilité de maintenir le trafic national en cas d'isolement. On verra quelles sont les méthodes employées par la Fédération russe pour pratiquer cet isolement.

fluvial (Rosmorrechflot) et la *Federal State Unitary Enterprise* (FSUE, Rosmorport)⁹¹⁷. Par ailleurs, comme on le verra, la plupart des autres câbles sous-marins russes sont gérés ou cogérés par le plus grand FAI russe, Rostelecom dont l'État est le propriétaire principal à travers l'Agence Fédérale pour la gestion des biens de l'État – la Rosimushchestvo détentrice de 38% des parts de Rostelecom⁹¹⁸.

On commence par étudier la centralisation de voies nationales d'accès pour chacun des réseaux nationaux comparés, avant d'examiner la centralisation des voies internationales. On évalue la centralisation des voies nationales à l'aide de trois critères : le nombre de câbles connectés au territoire (plus il est faible, moins les voies sous-marines d'accès sont diversifiées, plus le réseau est centralisé par un petit nombre de câbles) ; la diversité de la gestion des câbles sous-marins (moins la gestion des voies sous-marines est diversifiée, plus le réseau est centralisé par un petit nombre de gestionnaires différents) ; et l'étatisation du réseau sous-marin (plus la gestion du réseau est étatisée, plus le réseau est centralisé par la puissance publique).

	Critère 1 : nombre de câbles sous-marins connectés au territoire national
États-Unis	89
Royaume-Uni	58
France	27
Russie	9
Chine	19

S'agissant du nombre de câbles connectés au territoire, le réseau russe est de loin le plus centralisé par le nombre des câbles sous-marins qu'il connecte (9) : il est deux fois plus centralisé que le réseau chinois (19), trois fois plus que le réseau français (27), six fois plus que le réseau britannique (58) et presque dix fois plus que le réseau américain (89). Cela signifie que les résidents russes peuvent emprunter un faible nombre de voies d'accès sous-marines – 9 – pour communiquer entre eux. Dans le tableau ci-contre, on a entouré en bleu foncé le réseau le plus centralisé, et en plus clair le réseau le plus décentralisé d'après le critère du nombre de câbles rattachés au territoire.

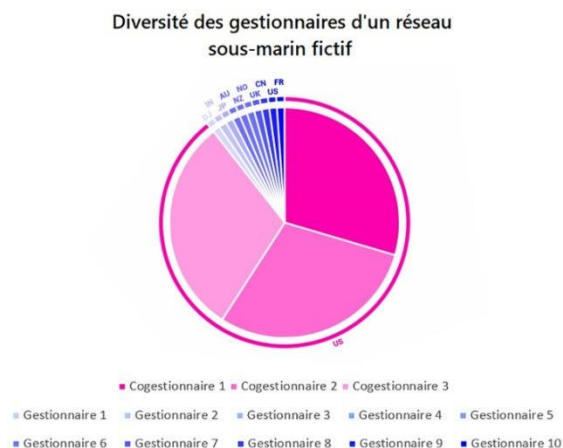
S'agissant de la diversité des gestionnaires, deux catégories d'acteurs doivent être distingués sur le marché des câbles sous-marins : les fournisseurs des infrastructures de câbles

917V. fiche du Polar Express sur la base de données Submarine Networks

918« Digital Ministry opposes giving state's stake in Rostelecom to Rostec, sees risks as too high - source », *Interfax.com* [journal russe], avr. 2022

(l'opérateur américain SubCom, l'opérateur français Alcatel Submarine Networks, l'opérateur chinois HMN (Huawei)...); et les investisseurs des câbles, qui sont propriétaires et gestionnaires des câbles et de leurs points d'atterrissage (stations dans lesquelles un câble sous-marin touche terre). La plupart des investisseurs sont des opérateurs de transmission : Orange (FR), TelecomEgyt (EG), AT&T (US), Verizon (US), China Telecom (CN), BT (UK), Tata Communications (IN), Chunghwa Telecom (TW), Singtel (SG)... Les opérateurs de transmission ne sont toutefois pas les seuls intéressés par le marché des câbles sous-marins et on y compte aussi des acteurs habituellement situés sur le marché logiciel (Google, Meta (ex-Facebook), Microsoft...), des banques d'investissement (Softbank (JP), Leucadia National Corp. (US), I Squared Capital (US)...), ou encore des entreprises spécialement créées pour la pose et la gestion d'un câble et dont le projet est souvent financé par des banques (Quintillion (US), Confluence Networks (US)...).

En raison de son mode de gestion, le câble sous-marin peut répondre à deux modes de propriétés. D'abord, si le câble n'est soutenu que par un investisseur, il appartient à un seul propriétaire qui le gère exclusivement : c'est le cas du câble FLAG Atlantic-1 appartenant exclusivement à l'opérateur britannique Global Cloud Xchange et reliant la France, les États-Unis et le Royaume-Uni, qui, ou encore du câble Glo-1 appartenant exclusivement à l'opérateur nigérian Globacom Ltd. et reliant le Royaume-Uni, le Nigéria et le Ghana, ou du câble EAC-C2C appartenant exclusivement à l'opérateur australien Telstra et reliant la Chine, le Japon, les Philippines, Singapour, la Corée du Sud et Taïwan. Ensuite, si le câble est soutenu par plusieurs investisseurs, il appartient à un consortium de co-propriétaires qui le gèrent collectivement : le câble New Cross Pacific, qui relie la Chine, les États-Unis, le Japon, la Corée du Sud et Taïwan, appartient collectivement à China Mobile, China Telecom, China Unicom (CN), Chunghwa Telecom (TW), KT (KR), Microsoft (US) et Softbank (SG) ; le câble Asia Submarine-cable Express/Cahaya Malaysia, qui relie la Chine, le Japon, la Malaisie, les Philippines et Singapour, est collectivement géré par les opérateurs japonais NTT, philippin PLDT, singapourien Starhub et malaisien Telekom Malaysia. Le consortium peut à cette fin créer une entreprise commune dédiée à la gestion du câble : le consortium propriétaire du câble PEACE a créé l'entreprise Peace Cable International Network Co. Ltd. qui regroupe les opérateurs PCCW Global (HK), Cybernet (PK), Djibouti Telecom (DJ), Golis Telecom Somalie (SO), Hormuud Telecom (SO), Interxion (NL) et Telkom Kenya (KE) pour gérer ce câble qui relie la France, Malte, Chypre, l'Égypte, Djibouti, la Somalie, le Kenya, les Seychelles, le Pakistan, les Maldives et Singapour ; de même, le consortium propriétaire du câble JUNO a créé l'entreprise Seren Juno Network Co. Ltd. qui regroupe les opérateurs NTT (JP) et Mitsui (JP) et la société de crédit-bail JA Mitsui Leasing SA (JP) pour gérer ce câble reliant le Japon, les États-Unis et la Corée du Sud.

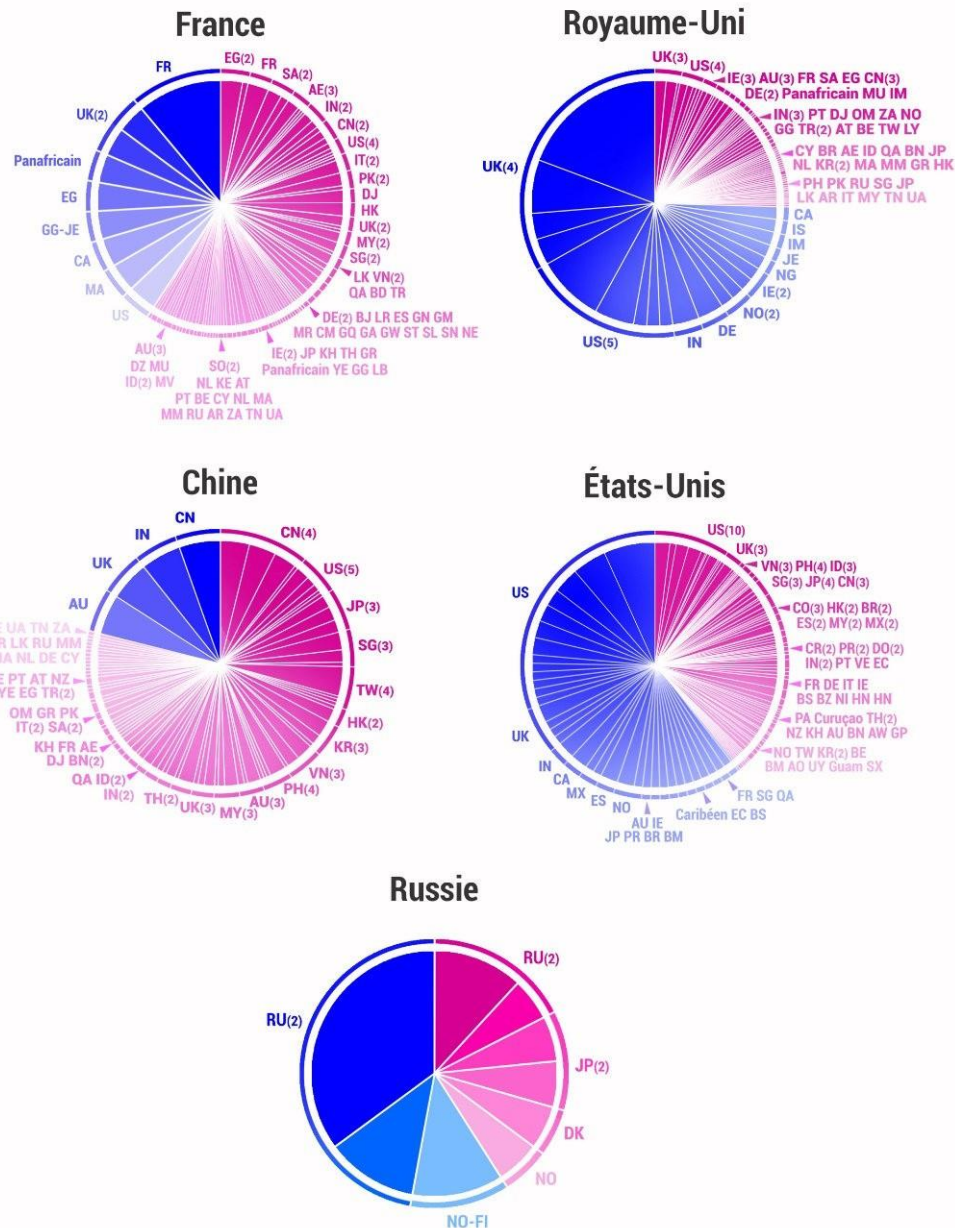


Un réseau sous-marin national peut donc comporter à la fois des câbles gérés exclusivement et des câbles cogérés. *A priori*, la cogestion semble déboucher sur une gestion plus décentralisée du réseau sous-marin car une pluralité de propriétaires se partagent la gestion des câbles, par opposition à la gestion exclusive revenant à un seul propriétaire d'un ou plusieurs câbles. À l'échelle d'un réseau, tel n'est pas nécessairement le cas en théorie. Dans le graphique ci-contre, on représente un réseau sous-marin national fictif dont 10% des câbles sont gérés exclusivement

(parts de couleur bleue) et dont 90% des câbles sont cogérés (parts de couleur rose). Dans notre réseau sous-marin fictif, seuls trois cogestionnaires (par ex. AT&T, Verizon et Google) se partagent tous les câbles cogérés. Ces trois cogestionnaires sont par ailleurs d'une même nationalité (US), de sorte que 90% des câbles de ce réseau sont cogérés par seulement trois cogestionnaires d'une même nationalité. En revanche, 10% des câbles sont gérés par 10 gestionnaires de 10 nationalités différentes (française, américaine, chinoise, britannique, norvégienne, birmane, australienne, japonaise, indienne et djiboutienne). Cela signifie que la gestion exclusive des câbles de ce réseau est plus diversifiée que leur gestion collective. Dans ce cas, le fait que la majorité des câbles soit cogérée n'est pas gage d'une importante diversité des gestionnaires : le réseau est essentiellement diversifié à travers la gestion exclusive des câbles sous-marins, tandis que la cogestion est au contraire le moyen d'une forte centralisation de la gestion du réseau sous-marin national. La cogestion peut être un instrument de centralisation, et ne signifie donc pas en elle-même que le réseau serait décentralisé. On en déduit qu'**un réseau sous-marin dont la majorité des câbles serait gérée collectivement n'est pas, de ce seul fait, plus décentralisé qu'un réseau sous- marin dont la majorité des câbles serait gérée exclusivement.**

Pour évaluer à quel point la gestion d'un réseau sous-marin est centralisée, le mode de gestion (exclusif ou collectif) est alors un paramètre qui doit être relativisé par le nombre de gestionnaires et de cogestionnaires de ce réseau ainsi que par le nombre de leurs nationalités. On a représenté ci-après la diversité de gestion des réseaux sous-marins français, russe, américain, chinois et britannique incluant ces divers paramètres :

Diversité de la gestion des réseaux sous-marins nationaux



Ces graphiques nous permettent de visualiser la diversité des gestionnaires de câbles des réseaux sous-marins comparés, tant concernant le nombre de gestionnaires que leur nationalité. Le cercle représente la totalité des câbles constitutifs du réseau sous-marin. Chaque part du cercle représente un gestionnaire ou un cogestionnaire différent. Chaque part détenue par un gestionnaire exclusif (en bleu) est proportionnelle au nombre de câbles qu'il gère exclusivement. De même, chaque part détenue par un cogestionnaire (en rose) est proportionnelle au nombre de câbles qu'il cogère. Pour chacun des graphiques, les filiales (Orange Polska, Orange Cameroon, Level3, Altibox...) ont été incluses dans les parts détenues par leurs maisons-mères (Orange, Lumen, Telia...). On en tire les informations comparatives suivantes :

Critère 2 : diversité de la gestion des câbles sous-marins	États-Unis	Royaume-Uni	France	Chine	Russie
Nombre total de gestionnaires exclusifs	35	20	9	4	3
Nombre de nationalités parmi les gestionnaires exclusifs	18	11	8	4	2
Nombre total de cogestionnaires	86	65	88	81	6
Nombre de nationalités parmi les cogestionnaires	49	50	64	45	4

À nouveau, les réseaux les plus centralisés par leur gestion (*i.e.* dont la gestion est la plus diversifiée) ont été entourés en bleu foncé. On constate que la Russie est le réseau sous-marin dont la gestion est la plus centralisée, tant sur la gestion exclusive que sur la gestion collective de ce réseau. Cela implique que la gestion du réseau sous-marin russe dépend d'un petit nombre d'acteurs, par ailleurs peu diversifiés dans leurs nationalités (au total, 8 gestionnaires *et* cogestionnaires différents de 4 nationalités différentes). Cette dépendance du fonctionnement du réseau sous-marin à quelques gestionnaires signifie que tous les utilisateurs du réseau dépendent eux-mêmes d'un petit nombre de gestionnaires pour voir leurs données transportées par voie sous-marine. Inversement, les réseaux les plus décentralisés par leur gestion ont été entourés en bleu clair. On remarque à ce propos un fait intéressant : tandis que le réseau sous-marin américain est celui dont la gestion exclusive des câbles est la plus décentralisée, c'est dans le réseau sous-marin français que la gestion collective des câbles est la plus décentralisée (par le nombre de cogestionnaires mais surtout par le nombre de nationalités impliquées). On remarque par ailleurs que le réseau sous-marin chinois est très décentralisé par sa cogestion, d'autant que la part de câbles cogérés représente 78.94% de la totalité des câbles constitutifs du réseau.

Jusqu'à présent, on a vu que le réseau sous-marin russe est le plus centralisé, tant par le nombre de câbles constitutifs de son réseau que par la diversité de leurs gestionnaires. On évalue la centralisation des réseaux sous-marins nationaux à partir d'un troisième critère : la mesure dans laquelle le réseau est étatisé. En effet, si l'État est directement ou indirectement propriétaire des gestionnaires du réseau, cette propriété fait de l'État un chef de gestion de câbles, de façon qu'une pluralité de gestionnaires est rapportable à un seul et même supra-gestionnaire – l'État. Autrement dit, l'étatisation des voies d'accès à un réseau ne peut pas provoquer une diversification et donc une décentralisation de ce réseau, mais seulement une unification du réseau et donc une centralisation de ses voies d'accès. Une appropriation par un seul et même acteur privé de tous les gestionnaires aurait le même effet centralisateur, le point déterminant de la centralisation n'étant pas le caractère privé ou public du propriétaire mais son unité. On considère que l'État s'approprie directement un gestionnaire si l'un au moins des pouvoirs publics (classiquement exécutif, législatif ou judiciaire) gère lui-même un câble sous-marin. C'est le cas du Polar Express en Russie, directement géré par le gouvernement. On considère que l'État s'approprie indirectement un gestionnaire si l'un au moins des pouvoirs publics est le principal actionnaire (par ex. l'opérateur Rostelecom en Russie) voire l'actionnaire majoritaire (par

ex. China Telecom, China Unicom et China Mobile en Chine) des gestionnaires de câbles. On répertorie les données suivantes sur l'étatisation des réseaux sous-marins :

Critère 3 : étatisation du réseau sous-marin	US	UK	FR	CN	RU
Proportion des câbles gérés exclusivement qui appartiennent directement à l'État	3.55%	0%	0%	0%	20%
Proportion des câbles gérés exclusivement qui appartiennent indirectement à l'État	0%	0%	27.27%	25%	60%
Proportion des câbles gérés collectivement qui appartiennent directement à l'État	0%	0%	0%	0%	0%
Proportion des câbles gérés collectivement qui appartiennent indirectement à l'État	0%	0%	4.65%	13.78%	28.73%
Proportion totale des câbles du réseau qui appartiennent directement ou indirectement par l'État	2.24%	0%	13.86%	16.12%	56.9%

On remarque d'abord que le réseau sous-marin britannique est le moins étatisé d'entre tous : aucun câble sous-marin ne relève d'un gestionnaire qui appartiendrait directement ou indirectement à l'État. Aux États-Unis, le gouvernement fédéral gère exclusivement et directement deux câbles, soit 3.55% de la totalité des câbles gérés exclusivement : le câble GTMO-1 qui relie la Floride à la baie cubaine de Guantanamo (où se situe une prison américaine incarcérant des combattants ennemis des États-Unis capturés par l'armée américaine dans le cadre d'opérations à l'étranger), et le câble GTMO-PR qui relie la baie de Guantanamo à un point d'atterrissage géré par le gouvernement américain sur la plage états-unienne de Punta Salinas à Porto Rico. Toutefois, aucun câble n'appartient indirectement à la Fédération via un gestionnaire dont elle serait l'actionnaire principal ou majoritaire. En somme, les câbles gérés par l'État fédéral des États-Unis représentent 2.24% de la totalité des câbles constitutifs du réseau sous-marin.

En France, l'État ne gère aucun câble directement mais il est le principal actionnaire de la société Orange et possède 22.96% de son capital (en y incluant les 9.56% détenus par la Banque publique d'investissement)⁹¹⁹. À travers Orange, l'État est indirectement propriétaire et donc gestionnaire de 27.27% de la totalité des câbles gérés exclusivement. Par ailleurs, Orange cogère 4.65% de la totalité des câbles gérés collectivement. En somme, l'État est le gestionnaire indirect de 13.86% de la totalité des câbles constitutifs du réseau sous-marin. Quant à la Chine, à travers China Telecom, China Unicom et China Mobile, l'État est indirectement gestionnaire de 25%

⁹¹⁹ Profil de la société Orange sur Zonebourse.com

de la totalité des câbles gérés exclusivement (2.3% de moins qu'en France), et indirectement cogestionnaire de 13.78% de la totalité des câbles gérés collectivement (9% de plus qu'en France). En somme, l'État est le gestionnaire indirect de 16.12% de la totalité des câbles constitutifs du réseau sous-marin (2.26% de plus qu'en France). Au-delà de ces chiffres, la gestion étatique indirecte chinoise est néanmoins très différente de la gestion étatique indirecte française : en Chine, l'État est actionnaire majoritaire des trois gestionnaires à hauteur de plus de 70% du capital ; en France, non seulement l'État n'est pas actionnaire majoritaire mais surtout, la très nette majorité du capital (60%) est flottante (*i.e.* échangeable sur les marchés) et appartient à des investisseurs institutionnels telles de que des banques, des sociétés de gestion d'actifs ou encore des caisses de dépôts (Amundi Asset Management possède 8.72%, BNP Paribas possède 1.14%, The Vanguard Group possède 1.92%...). En d'autres termes, Orange obéit principalement à des acteurs privés, et la position de l'État en tant que premier actionnaire lui fournit le pouvoir de maintenir « *une minorité de blocage* »⁹²⁰ bien plus qu'un pouvoir de décision sur la direction de l'entreprise – lequel pouvoir de décision se partage essentiellement entre des intérêts privés. Par conséquent, le pouvoir de gérer indirectement les câbles sous-marins est sensiblement plus faible en France qu'en Chine, ne serait-ce que parce que le pouvoir de décision sur la direction de l'entreprise appartient indirectement à l'État en Chine tandis qu'il se partage entre une majorité d'intérêts privés en France.

Enfin, quel que soit le terrain sur lequel on évalue l'appropriation étatique des câbles sous-marins, le réseau sous-marin russe est à nouveau le plus centralisé selon ce critère. Le Polar Express directement géré par le gouvernement représente 20% de la totalité des câbles sous-marins gérés exclusivement ; et à travers l'opérateur Rostelecom, la Fédération gère 60% de la totalité des câbles sous-marins gérés exclusivement et cogère 28.73% de la totalité des câbles sous-marins gérés collectivement. En somme, la Fédération russe gère directement et indirectement 56.9% de la totalité des câbles constitutifs du réseau sous-marin.

Dans un réseau sous-marin national, les câbles peuvent être empruntés par toute machine située sur le territoire national pour accéder à une autre machine située sur le territoire national (accès nationaux). Les données provenant du territoire national circuleront alors à travers les câbles sous-marins pour revenir sur le territoire national à l'arrivée – parfois même sans l'avoir jamais quitté en empruntant des câbles qui connectent plusieurs stations du territoire (Polar Express en Russie, le câble H2HE en Chine, les câbles PC-1 ou Quintillon aux États-Unis, BIT Highlands and Islands Submarine Cable System au Royaume-Uni, les câbles Corse Contient 4 et 5 en France...). Les critères du nombre de câbles connectés au réseau national, de la diversité des gestionnaires et de l'étatisation du réseau indiquent combien ces accès nationaux sont centralisés dans un réseau sous-marin national. Toutefois, ils n'indiquent pas la diversité des voies internationales d'accès au réseau, *i.e.* la mesure dans laquelle le réseau national peut échanger avec des réseaux nationaux. Pour évaluer cette mesure, on s'appuie sur un quatrième critère de centralisation : la diversité des réseaux étrangers auxquels le réseau national est connecté. On obtient les données comparatives suivantes.

920« L'Etat entend rester “un des principaux actionnaires d'Orange”, assure Hollande », sur *Les Echos*, 8 juin 2016

Critère 4 : diversité des réseaux étrangers connectés au réseau national	US	UK	FR	CN	RU
Nombre de câbles sous-marins connectés au territoire national qui desservent des pays tiers	52	42	24	18	5
Nombre de pays tiers desservis par les câbles connectés au territoire	57	59	70	35	4

C'est en Russie que les réseaux étrangers connectés au réseau national sont le moins diversifiés, tant par le nombre de câbles sous-marins connectés à des réseaux étrangers que par le nombre de pays tiers connectés par voie sous-marine. Par conséquent, des cinq réseaux sous-marins étudiés, **le réseau russe est celui qui centralise le plus les voies de communication entre le réseau national et les réseaux étrangers**. On a vu par ailleurs qu'il est **aussi le réseau sous-marin qui centralise le plus les voies de communications au sein du réseau national**, tant par le nombre de câbles constitutifs du réseau national que par la diversité de leur gestion et par leur étatisation. S'ensuit la Chine qui arrive en deuxième position des réseaux sous-marins les plus centralisés parmi ceux étudiés, là encore au niveau des voies d'accès tant nationales qu'internationales. On souligne toutefois que cette deuxième position s'explique par l'échantillon des pays étudiés, et que le réseau sous-marin chinois est assez peu étatisé dans l'ensemble, que sa gestion y est diversifiée, que le nombre de câbles constitutifs du réseau n'est pas notablement restrictif et que les réseaux étrangers connectés par le réseau sous-marin chinois sont eux-mêmes assez diversifiés. En somme, le réseau sous-marin chinois est assez décentralisé. Les trois dernières positions se disputent entre la France, le Royaume-Uni et les États-Unis, qui sont alors les réseaux sous-marins nationaux les plus décentralisés au niveau des voies de communications tant nationales qu'internationales, par la privatisation de leur réseau-marin (Royaume-Uni), par le nombre total de câbles constitutifs du réseau national (États-Unis), par la diversité de leurs gestionnaires exclusifs (États-Unis) ou de leurs cogestionnaires (France), par le nombre de câbles constitutifs du réseau national connectés à des pays tiers (États-Unis) et par le nombre de pays ainsi desservis (France).

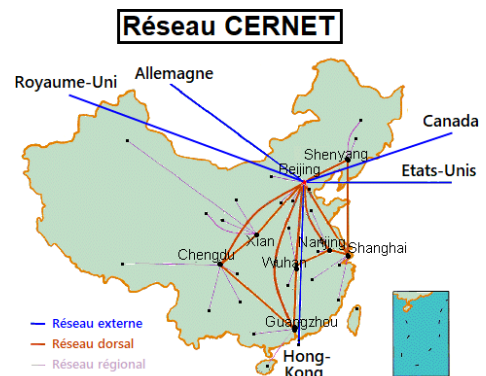
B) La centralisation de l'acheminement : métriques de la centralisation

La Chine fut précurseur dans le domaine de la centralisation de l'acheminement. Dès 1996, le Conseil d'État de la République populaire de Chine établit une scission entre le trafic national et le trafic international : « *les réseaux de communication informatique ne peuvent être connectés au réseau international qu'en utilisant les canaux internationaux d'entrée et de sortie fournis par le Réseau public national de télécommunications du ministère des Postes et télécommunications* »⁹²¹. Quatre ans plus tard, le Conseil d'État transfère au ministère de l'Industrie et des Technologies de l'information la compétence sur la gestion des canaux

⁹²¹ Conseil des affaires de l'État, Dispositions provisoires pour la gestion de la connexion internationale des réseaux informatiques (中华人民共和国计算机信息网络国际联网管理暂行规定), 1^{er} fév. 1996, art. 6

internationaux de communication informatique, et institue sous l'égide de ce ministère un Bureau d'entrée et de sortie des communications internationales chargé d'approuver l'exploitation commerciale de ces canaux⁹²².

En 1999, ce Bureau autorisait seulement quatre opérateurs à connecter leurs réseaux aux lignes internationales⁹²³ : China Telecom, avec son réseau dorsal ChinaNet (accès civil au réseau international) , premier réseau dorsal, ou « backbone », de Chine⁹²⁴ ; China Unicom et sa dorsale Netcom (accès civil au réseau international) ; l'Académie chinoise des sciences avec son réseau CSTNET (accès scientifique au réseau international) ; et le Ministère de l'Éducation, avec son réseau CERNET (plus grand réseau universitaire du monde, interconnectant les principales universités chinoises avec le réseau international). Par exemple, ci-contre, le réseau CERNET exploite au moins cinq canaux internationaux de sortie des communications, respectivement dirigés vers le Royaume-Uni, l'Allemagne, le Canada, les États-Unis et Hong-Kong.



* carte reprise et traduite depuis l'article de JIN Hai, MAO Feng et CHEN Hanhua, "P2P based decentralized dynamic replica placement strategy in data grid environment", *Girds Computing Lab [en ligne]*, 2015

Depuis 1999, au moins sept autres opérateurs se sont vus octroyés le droit de connecter leurs réseaux à des réseaux internationaux : les opérateurs China Mobile et Oriental Cable Network (OCN) et les entreprises Baidu, Tencent, NetEase, Alibaba et 21Vianet⁹²⁵. Appartenant majoritairement à l'État, China Mobile est un opérateur de transmission qui met ses infrastructures réseau à disposition de ses abonnés pour leur fournir un accès internet. OCN est également une entreprise d'État, l'un des plus grands opérateurs chinois spécialisé dans la pose de câbles et la transmission de programmes télévisés. Tencent, Alibaba, Baidu, NetEase et 21Vianet sont des fournisseurs d'hébergement à capitaux privés, qui mettent leurs serveurs à disposition des propriétaires d'applications (sites web, jeux vidéo en ligne, applications mobile...) contre rémunération afin d'héberger ces applications et donc de les rendre disponibles en ligne. On verra que les « géants » chinois Tencent, Alibaba, Baidu et NetEase hébergent de nombreuses applications parmi les plus populaires en Chine (WeChat, WeChat Pay, QQ, QQ Browser, Tencent Video, Baidu Search, Baidu Map, iQIYI, TaoBao, Alipay, Autonavi Map, NetEase Mail, NetEase Cloud Music...). La connexion directe de leur réseau de serveurs et de routeurs à des réseaux étrangers permet de faciliter l'accès depuis l'étranger aux services hébergés par les réseaux de Tencent,

922 Conseil des affaires de l'État, Règlement sur les télécommunications (中华人民共和国电信条例), 25 sept. 2000, art. 64

923 TAN Zixiang (Alex), FOSTER William et GOODMAN Seymour, « China's state-coordinated Internet infrastructure », *Communications of the ACM*, vol. 42, 1999, p. 44-52

924 Une dorsale est un concept abstrait indéfini et ambiguë scientifiquement, qui désigne un réseau d'un opérateur connectant les principaux routeurs du réseau (par ex. national) auquel il appartient.

925 Comme on le verra plus loin, ces opérateurs possèdent des réseaux de routeurs (i.e. des « autonomous systems », AS) qui sont connectés à des réseaux de routeurs (AS) étrangers. China Mobile est connecté au réseau international via son AS9808 intitulé « China Mobile Communications Group td », Tencent est connecté au réseau international via son AS13203 « Tencent Building », NetEase l'est via son AS135357 « Shenzhen Katherine Heng Technology Information Co. Ltd » et 21Vianet l'est via son AS58593 « Shangai Blue Cloud Technology ». Ces informations sont disponibles sur la base de données en ligne IPinfo.org, qui agrège les registres publics pour recenser les caractéristiques de chaque AS. Shenzhen Katherine Heng Technology Information Co. Ltd est une filiale de NetEase, Shangai Blue Cloud Technology est une filiale de 21Vianet.

Alibaba etc. On remarque que, tant du côté des opérateurs que du côté des fournisseurs d'hébergement, seules des entreprises chinoises sont à ce jour autorisées à offrir un accès international à internet.

Outre les cinq réseaux dorsaux ayant accès au réseau international (ChinaNet, Netcom, CMNET, CERNET et CSTNET), les huit autres réseaux dorsaux⁹²⁶ qui parcourent le territoire transmettent uniquement le trafic interne. Ils doivent s'interconnecter à l'une des cinq dorsales connectées à des réseaux étrangers pour fournir aux utilisateurs chinois l'accès à des services internationaux. Cette scission entre les réseaux dorsaux dédiés au trafic interne et les réseaux dorsaux faisant circuler le trafic international oblige le trafic national à ne jamais quitter le territoire, comme le rappelle une étude menée par le géant informatique Oracle⁹²⁷. Seules les requêtes ayant un destinataire étranger quittent le territoire national. Inversement, dans les autres pays, il est fréquent que le trafic national quitte régulièrement le territoire pour y revenir ensuite.

En somme, l'État centralise les canaux d'accès international au réseau internet de la façon suivante : les requêtes émises depuis la Chine ne peuvent accéder à des informations étrangères en ligne qu'en ayant pour destinataire l'un des six réseaux de transmission appartenant à l'État (ChinaNet, Netcom, CMNET, CSTNET, CERNET ou le réseau d'OCN) et le cas échéant l'un des cinq réseaux d'hébergement agréés par l'État (Tencent, Alibaba, Baidu, NetEase ou 21 Vianet). Par exemple, une application VPN doit nécessairement être hébergée par l'un de ces cinq réseaux d'hébergement pour fournir à ses utilisateurs chinois un accès internet hors de Chine. De même, les applications de Microsoft 365 accessibles en Chine (Word, Excel, PowerPoint, Outlook, OneDrive, Teams...) sont hébergées par 21Vianet⁹²⁸. Les utilisateurs chinois ne bénéficient donc que d'un très faible nombre de canaux pour accéder à des informations étrangères, et cet accès dépend de réseaux d'acheminement appartenant à l'État ou de réseaux d'hébergement certifiés par l'État et appartenant exclusivement à des entreprises chinoises. Les règles de 1996 et de 2000 du Conseil d'État créent dès le transport un goulot d'étranglement qui enferme l'accès à la R-DATA « informations étrangères » dans un petit nombre de voies d'accès⁹²⁹.

926Cinq de ces huit dorsales sont empruntables civilement : "China Telecom Next Generation Carrier Network" (CN2) et "China Telecom Data Center Interconnection" (DCI) appartenant à China Telecom, "China Industrial Internet" appartenant à China Unicom, "Réseau privé IP porteur" (IP 专用承载网) appartenant à China Mobile, CBNNET dédié au transport des signaux de radio et de télévision destiné à centraliser la transmission de ces signaux sur le territoire, et CITICNET appartenant à l'opérateur privé CTIC Ltd. assurant le développement de la fibre optique sur le territoire. Les deux autres dorsales sont réservées à des catégories spécifiques d'utilisateurs : CGWNET dédié au réseau militaire, CIETNET dédié au commerce extérieur et appartenant à l'autorité étatique du Centre international de commerce électronique de Chine. On totalise donc 13 dorsales dont cinq directement connectées au réseau international. V. NOAM Eli M., *Who Owns the World's Media?*, Oxford University Press, 2016, p. 758s. ; plus récemment, incluant CBNET né en 2019 et CITIC « Grand débrief sur les réseaux dorsaux de la Chine (Partie 2) » (大话中国骨干网 (下)), *Finance.sina.cn*, 12 déc. 2020

927CIMPANU Catalin, « Oracle: China's internet is designed more like an intranet », sur *ZDNet*, 23 juil. 2019

928« Office 365 operated by 21Vianet », sur *Learn.microsoft.com* [site officiel de Microsoft], 17 fév. 2023

929L'accès aux informations étrangères n'est pas interdit en Chine, mais on voit bien ici qu'il est restreint par la limitation du nombre de canaux d'accès. On qualifie donc l'accès aux « informations étrangères » comme une R-DATA en Chine dès lors qu'il fait l'objet d'une technique de restriction (centralisation)

Comment mesurer la centralisation du réseau chinois de l'acheminement pour la comparer avec la centralisation des autres réseaux nationaux d'acheminement ? En 2011, le Berkman Center for Internet & Society de l'Université de Harvard propose deux outils pour mesurer la centralisation de la transmission internet dans un pays⁹³⁰. Ces deux outils reposent sur le concept de « système autonome » (*autonomous system*, AS). Un AS est un réseau fourni par un ou plusieurs opérateurs dont les routeurs acheminent le trafic selon les mêmes caractéristiques de routage. À échelle mondiale, plus de 110 000 AS étaient répertoriés dans les bases de données des divers registries, dont 29 571 aux États-Unis (26.6% des AS dans le monde, en première position), 6 404 en Chine (5.7%, en troisième position derrière le Brésil), 5 883 en Russie (4.7%, en quatrième position), 19 595 dans l'Union Européenne (17.6%, avec, pour les deux premiers pays européens, l'Allemagne et ses 3027 AS en septième position puis la Pologne et ses 2571 AS en dixième position)⁹³¹.

TABLE III. COMPLEXITY BY REGION

Region	Average Complexity	Total IPs
Southern Africa	0.83	13,807,378
Eastern Asia	1.54	510,641,820
Central America	2.63	21,342,440
South America	2.64	64,518,477
Western Europe	3.31	155,311,961
Northern America	3.35	44,085,103
South-Eastern Asia	3.83	38,019,138
Australia & New Zealand	4.71	43,407,381
Western Asia	5.14	28,887,731
Southern Europe	5.24	69,446,080
Northern Europe	5.34	99,405,852
South Central Asia	6.78	26,635,456
Eastern Europe	11.35	74,574,504

* Tableau issu de ROBERTS H., LAROCHELLE D., FARIS R. et PALFREY J., « Mapping Local Internet Control » [en ligne], Berkman Center for Internet & Society, 2011, p. 9

Le premier outil du Berkman Center mesure la « complexité d'un réseau » en calculant le nombre d'adresses IP déclarées dans un pays par rapport au nombre d'AS dans ce pays. Moins il y a d'AS sur le territoire par rapport au nombre d'adresses IP, moins le réseau est complexe, plus son score de complexité sera faible, plus le réseau national sera centralisé par un faible nombre d'AS. *A contrario*, plus il y a d'AS par rapport au nombre d'adresses IP, plus le réseau est complexe, plus son score de complexité sera élevé, plus le réseau national sera décentralisé par un grand nombre d'AS⁹³².

930ROBERTS Hal, LAROCHELLE David, FARIS Robert et PALFREY John, « Mapping Local Internet Control » [en ligne], Berkman Center for Internet & Society, 2011

931« Regional Internet Registries Statistics - ASN statistics », sur Public.imtbs-tsp.eu [consulté le 31 août 2022]. Patrick Maignon, Professeur associé à Telecom SudParis Évry-Courcouronnes, tient ce site web pour mettre régulièrement à jour les bases de données des cinq registries.

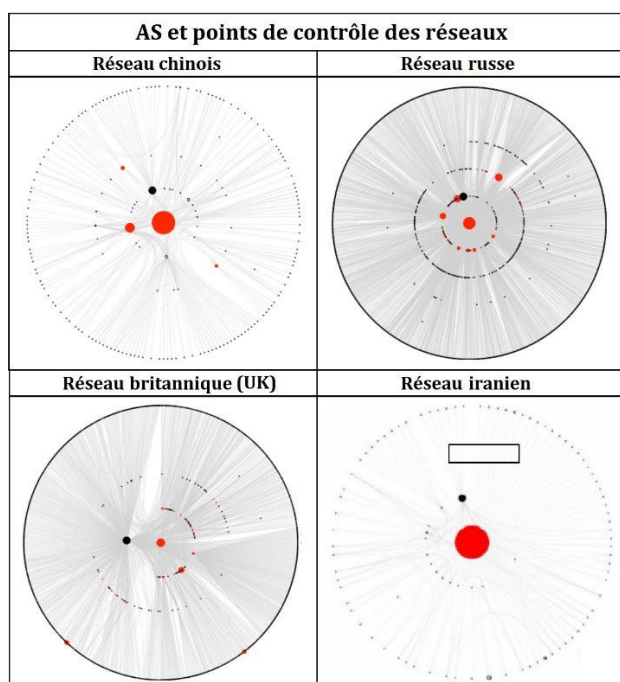
932D'après l'outil proposé, la complexité d'un réseau = $(AS/I) * \sum [CI(a)/I]$ où AS est le nombre total d'AS dans le pays, I le nombre total d'adresses IP dans le pays, $\sum$ la somme pour chaque AS dans le pays et CI(a) les adresses IP connectées à cet AS : v. p.13

La deuxième métrique développée par le Berkman Center est le « point de contrôle ». Les auteurs définissent le point de contrôle comme « *le plus petit ensemble d'AS qui connecte 90% des adresses IP du pays* »⁹³³. Par exemple, en 2011 dans la région de l'Asie de l'Est (Chine, Japon, Corées, Taïwan, Viêt-Nam...), en moyenne seuls 4.8 AS de la région connectaient 90% des 510 641 820 adresses IP déclarées dans cette région. En 2011, il existait donc en moyenne 4.8 points de contrôle du réseau dans cette région à partir des AS. Dans l'Europe de l'Est, en moyenne 19.1 AS de la région connectaient 90% des 74 574 504 adresses IP – on comptait donc 19.1 points de contrôle dans cette région etc.

TABLE II. AVERAGE POINTS OF CONTROL BY REGION

Region	Average PoC	Total IPs
South Central Asia	2.85	26,635,456
Central America	3.00	21,342,440
Western Asia	3.21	28,887,731
South America	4.40	64,518,477
Eastern Asia	4.80	510,641,820
Southern Africa	6.00	13,807,378
South-Eastern Asia	6.50	38,019,138
Southern Europe	6.55	69,446,080
Australia & New Zealand	7.50	43,407,381
Northern Europe	11.00	99,405,852
Western Europe	13.29	155,311,961
Northern America	14.00	44,085,103
Eastern Europe	19.10	74,574,504

*Source : *ibid.*



Moins il y a de points de contrôle (3 en Chine, 2 en Algérie et au Pakistan, 1 en Syrie et à Macao... en 2011), moins il y a d'AS nécessaires à la connexion de 90% des adresses IP, plus le réseau est centralisé par le faible nombre d'AS essentiels. Plus il y a de points de contrôle (48 en Ukraine, 37 en Suède, 32 en Bulgarie, 31 en République Tchèque, 19 en Russie et en Pologne... en 2011), plus il y a d'AS nécessaires à la connexion de 90% des adresses IP, plus le réseau est décentralisé par le grand nombre d'AS essentiels⁹³⁴. Dans les schémas ci-contre, les chercheurs ont représenté les réseaux de plusieurs pays à travers le nombre d'AS dans ce pays (chaque point, de taille variable), les relations de fourniture entre deux AS (lignes grises), le nombre d'AS étrangers (nœuds noirs) et le nombre de points de contrôle (nœuds rouges).

En 2021, une équipe de géographes, informaticien et mathématicien propose d'exprimer en pourcentage le rapport entre les points de contrôle et l'ensemble des AS d'un territoire (nombre total de points de contrôle sur un territoire / nombre total d'AS sur ce territoire). Les auteurs appellent « valeur de contrôle » le résultat de cette opération. « *Par exemple, si un pays A possède 300 AS et si 30 AS connectent 90% des adresses IP déclarées, alors la taille des points de contrôle*

⁹³³ROBERTS H., ZUCKERMAN Ethan, FARIS R., YORK Jillian et PALFREY J., *The Evolving Landscape of Internet Control* [en ligne], Berkman Center for Internet & Society, août 2011, p. 6

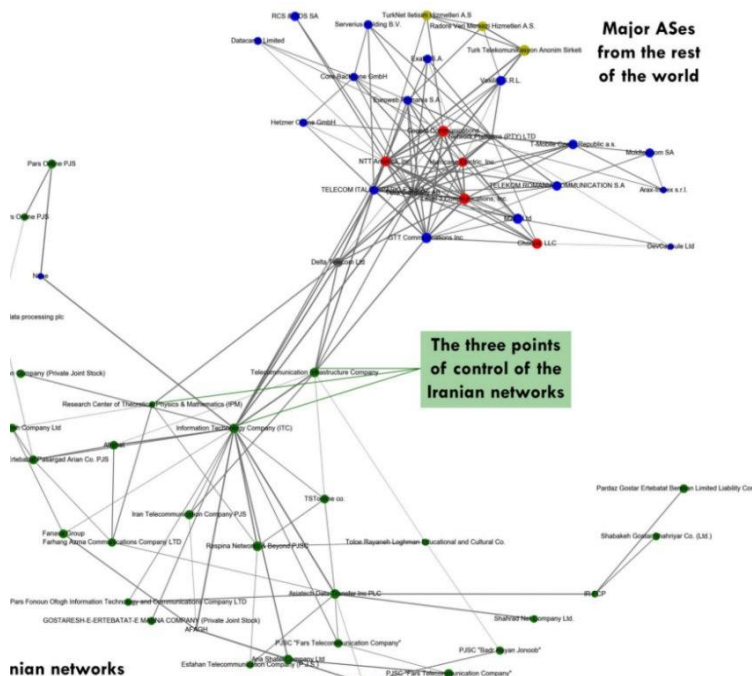
⁹³⁴À titre comparatif, les chercheurs avaient dénombré 7 points de contrôle en France et en Italie, 19 en Allemagne, 13 au Royaume-Uni, 10 en Espagne, 24 aux Pays-Bas, 11 en Grèce...

est de 30 et la valeur de contrôle est de $30/300 = 10\%$. »⁹³⁵. En l'espèce, la valeur de contrôle indique que 10% des AS sur le territoire sont essentiels, i.e. que 10% des AS sont nécessaires pour connecter 90% des adresses IP. « Plus la valeur de contrôle est basse, plus le réseau est centralisé » par sa faible proportion d'AS essentiels. Plus la valeur de contrôle est élevée, plus le réseau est décentralisé par sa forte proportion d'AS essentiels. Tandis que la complexité du réseau indique la centralité de certains AS par rapport au nombre total d'adresses IP déclarées, le point de contrôle indique la centralité de certains AS par rapport à l'essentiel des adresses IP déclarées, et la valeur de contrôle indique la centralité de certains AS par rapport à tous les AS d'après le nombre d'adresses IP qu'ils connectent.

Pour donner un aperçu de la structure d'acheminement du réseau iranien, les chercheurs explorent ses AS et observent l'existence de trois points de contrôle, dont seulement deux – Information Technology Company (ITC, AS12880) et Telecommunication Infrastructure Company (TIC, AS48159) – connectent l'ensemble du réseau iranien aux réseaux étrangers. « ITC est sous l'autorité du ministère iranien des Technologies de l'information et de la communication et TIC est directement affiliée à ITC. Cela montre que l'Iran a construit une architecture autour de l'idée d'un Internet national autosuffisant, connecté à l'internet mondial par deux AS hautement contrôlés. »⁹³⁶. On retrouve à nouveau la configuration de goulot d'étranglement propre à la technique de centralisation de l'accès telle qu'on l'a définie. En comparant ces données avec celles obtenues pour les autres pays du Moyen-Orient, les auteurs laissent voir, dans la plupart de ces pays, un important mouvement de centralisation du nombre d'AS par rapport au nombre d'adresses IP entre 2011 et 2019 (complexité du réseau) : cette intensification centralisatrice est très forte au Bahreïn, au Koweït, en Arabie Saoudite, en Égypte, en Syrie, à Oman ou encore au Qatar, elle est plus relative au Liban, en Irak, en Israël ou encore en Turquie. En revanche, entre 2011 et 2018, plusieurs pays ont connu une décentralisation du nombre d'AS essentiels (valeur de contrôle) : au Liban, en Iran, en Syrie, en Arabie Saoudite, en Israël ou encore en Turquie, a augmenté dans des mesures variables la proportion d'AS qui connectent 90% des adresses IP. Au contraire, on observe une centralisation du nombre d'AS essentiels dans d'autres pays : à Oman, en Irak, en Syrie, au Bahreïn ou encore au Qatar.

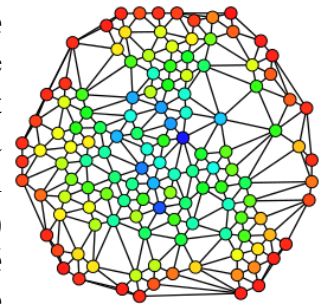
935SALAMATIAN Loqman, DOUZET Frederick, LIMONIER Kevin et SALAMATIAN Kavé, « The geopolitics behind the routes data travels: a case study of Iran », *Journal of Cybersecurity*, vol. 7, 2021, p. 13

936Ibid., p. 9



Country	Complexity		Control value		Number of ASes	
	2011	2019	2011	2018	2011	2019
Iran	3.82	3.75	2%	34%	96	437
Saudi Arabia	3.74	0.43	5%	10%	66	139
Iraq	6.46	4.93	75%	55%	4	107
Oman	1.06	0.05	50%	25%	2	12
Syria	0.85	0.00	33%	50%	3	2
Bahrain	10.20	0.26	22%	37%	18	19
Kuwait	4.70	0.52	20%	17%	30	61
Egypt	1.25	0.04	8%	9%	36	58
Afghanistan	NA	4.14	NA	52%	NA	46
UAE	0.58	0.31	20%	20%	8	65
Turkey	2.72	2.67	1%	7%	226	450
Israel	3.24	2.41	2%	10%	165	251
Qatar	1.55	0.02	40%	29%	5	9
Lebanon	11.99	7.81	22%	42%	32	133

Les AS centraux ne sont pas toujours identifiés à partir du nombre d'adresses IP qu'ils connectent avec pour repère les « points de contrôle connectant 90% des adresses IP ». Trois autres outils sont principalement utilisés pour identifier des AS centraux. D'après la mesure de la « centralité intermédiaire » (*betweenness centrality*), la centralité d'un AS peut être évaluée par le nombre de routes (« liens ») qui séparent cet AS de chaque autre AS lorsque l'AS dont la centralité est mesurée emprunte les routes les plus courtes⁹³⁷. D'après la mesure de la « centralité de proximité » (*proximity centrality*), la centralité d'un AS peut être évaluée par la somme de la distance des routes qui séparent cet AS de chaque autre AS lorsque l'AS dont la centralité est mesurée emprunte les routes les plus courtes⁹³⁸. Enfin, d'après la mesure de la « centralité de degré » (*degree centrality*), la centralité d'un AS peut être évaluée par le nombre de routes rattachées à cet AS⁹³⁹. Quelles que soient les



937FREEMAN Linton C., « A Set of Measures of Centrality Based on Betweenness », *Sociometry*, vol. 40, American Sociological Association, Sage Publications, 1977, p. 35-41. La formule de calcul de la centralité intermédiaire est $\sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$ où $\sigma_{st}(v)$ est le nombre de chemins les plus courts de s à t , et

$\sigma_{st}(v)$ est le nombre de ces chemins passant par le vecteur v .

938BAVELAS Alex, « A mathematical model for group structures », *Applied Anthropology*, 7, Society for Applied Anthropology, 1948. La formule de calcul de la centralité de proximité est $\frac{1}{\sum_{y \neq x} d(y, x)}$

où $d(y, x)$ est la distance du chemin le plus court entre x et y . Pour approfondir la manipulation de cet algorithme, v. COHEN Edith, DELLING Daniel, PAJOR Thomas et WERNECK Renato F., « Computing Classic Closeness Centrality, at Scale » [en ligne], *Proceedings of the second edition of the ACM conference on Online social networks - COSN '14*, août 2014

939La centralité du degré a pour dérivés : la « centralité des vecteurs propres » (*eigenvector centrality*) qui prend en compte la qualité de connexion des nœuds et le nombre de liens que possèdent les nœuds connectés au nœud mesuré ; et l'algorithme PageRank qui s'appuie sur la centralité des vecteurs propres, en la complétant par le poids d'influence de chaque lien et par la direction du trafic (l'influence est-elle transmise du nœud A vers le nœud B, ou du nœud B vers le nœud A ?). Ces algorithmes sont généralement utilisés pour mesurer les jeux d'influence sur les réseaux sociaux, v. par ex. HANSEN Derek L., SHNEIDERMAN Ben, SMITH Marc A. et HIMELBOIM Itai, « Chapter 3 - Social network analysis », *Analyzing Social Media Networks with NodeXL (Second Edition)*, Morgan Kaufmann, 2020, p. 31-51

caractéristiques retenues pour calculer la centralité d'un AS (nombre d'adresses IP qu'il connecte, nombre de routes les plus courtes, distance des routes les plus courtes...), quelle que soit la méthode employée (centralisation des canaux internationaux en Chine et en Iran, centralisation des moyens de transport sous-marins en Russie...), la centralisation s'inscrit toujours dans la configuration d'un petit nombre de nœuds destinataires qui concentrent les requêtes d'un grand nombre de nœuds émetteurs.

C) La centralisation de l'acheminement : comparaisons internationales

1. Comparaison des réseaux nationaux d'acheminement

On a examiné comment et combien un réseau national de transport sous-marin pouvait être centralisé. On s'intéresse désormais à une comparaison de quatre réseaux nationaux d'acheminement : la Chine, la France, la Russie et le Royaume-Uni. À nouveau, on applique notre définition du réseau national de transmission comme étant l'ensemble des moyens de transmissions présents sur un territoire national. À la différence d'un réseau national de transport, les moyens de transmission d'un réseau national d'acheminement ne sont plus des moyens de transport (tels que des câbles sous-marins) mais des moyens d'acheminement, *i.e.* des routeurs présents sur le territoire. Comme pour le réseau sous-marin, on analysera distinctement la centralisation des accès nationaux (échanges entre deux machines présentes sur le territoire) et la centralisation des accès internationaux (échanges entre une machine présente sur le territoire et une machine connectée à un réseau étranger).

Pour mesurer la centralisation de l'acheminement, on s'appuie sur le repère du nombre de « points de contrôle », considéré comme le nombre d'AS nécessaires à la connexion de 90% des adresses IP du réseau national. Faute d'avoir trouvé des travaux scientifiques ayant étudié en 2022 les points de contrôle des réseaux nationaux ici comparés, on soumettra nos propres résultats en employant la méthode du Berkman Center. Afin d'identifier les points de contrôle, il est nécessaire de connaître le nombre total d'adresses IP attribuées dans un réseau national et le nombre d'adresses IP attribuées à chaque AS – par ex., dans le réseau d'acheminement français, le plus gros AS appartient à Orange (AS3215) et se voit attribuer par l'Icann le contrôle de 20 111 104 adresses IP qu'Orange peut ensuite réattribuer à ses clients, tandis que le dixième plus gros AS appartient à Free (AS12876, Scaleway filiale d'Iliad) et se voit attribuer 475 136 adresses IP. On obtient ces informations sur la base de données [IPInfo.io](https://ipinfo.io) qui actualise régulièrement les informations relatives aux AS (AS d'un pays, nombre d'adresses attribuées par AS, connexions entre AS...), et qu'on a croisé avec la base de données homologue bgp.he.net fournie par l'opérateur tier 1 Hurricane Electric pour confirmer des informations.

À l'aide de la base IP Info, en octobre 2022, on dénombre 343 009 060 adresses IP attribuées au réseau chinois, 79 542 016 au réseau britannique, 74 121 979 au réseau français et 47 049 216 au réseau russe. En Chine, le seuil des 90% des adresses IP (soit 308 708 154 adresses IP) est atteint par les 27 plus gros AS. Autrement dit, sur les 548 AS recensés par IP Info dans le réseau chinois, seuls 27 AS sont nécessaires pour connecter 90% des adresses IP. Cela signifie qu'on compte 27 points de contrôle, 27 AS dont le contrôle couvre 90% des adresses IP du réseau national. En France, le seuil des 90% est atteint par les 29 plus gros AS, ce qui représente 29 points de contrôle sur les 1 276 AS recensés par IP Info. On identifie 82 points de contrôle pour 1 948 AS au Royaume-Uni, et en Russie, et pas moins de 767 points de contrôle pour 4 982 AS en Russie – 767 AS y sont donc nécessaires pour connecter 90% des adresses IP du réseau national. En 2011, le Berkman Center comptait 3 points de contrôle en Chine, 7

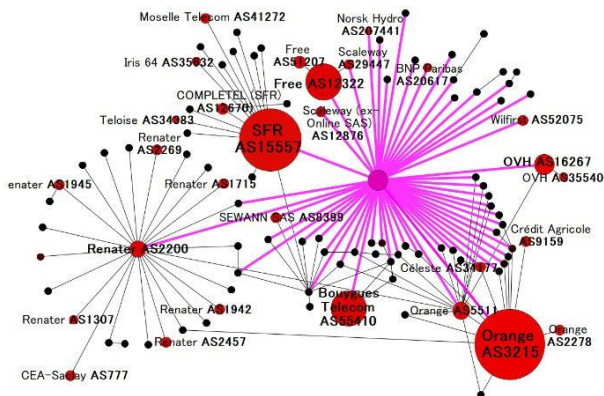
en France, 13 au Royaume-Uni et 19 en Russie. Depuis 2011, on relève donc une forte augmentation du nombre de points de contrôle dans tous les réseaux nationaux étudiés.

On explique cette augmentation du nombre de points de contrôle par l'accroissement du nombre d'adresses IP depuis 2011 dû à l'essor de la technologie *cloud* (qui conduit à l'apparition de nouveaux fournisseurs *cloud* gérant les AS de leurs datacenter⁹⁴⁰), au développement de l'accès internet dans les entreprises, et à l'expansion d'opérateurs régionaux (principalement en Russie et en France) et nationaux (notamment en Chine) pour couvrir le territoire d'un accès internet. La hausse du nombre d'adresses IP attribuées depuis 2011 rehausse mécaniquement le nombre d'adresses IP incluses dans le seuil des 90% d'adresses IP, ouvrant ainsi à un plus grand nombre d'AS la possibilité d'intégrer les AS nécessaires à la connexion de 90% des adresses IP et donc de devenir des points de contrôle. Par exemple, dans un réseau de 100 adresses IP, l'AS1 attribue 90 adresses IP et l'AS2 en attribue 10, de façon que l'AS1 concentre 90% des adresses IP et représente le seul point de contrôle. L'année suivante, un nouvel AS – l'AS3 – qui attribue 5 adresses IP intègre le réseau, rehaussant à 105 le nombre total d'adresses IP dans le réseau. Le seuil des 90% ne couvre plus les 90 adresses attribuées à l'AS1 dans un réseau des 100 adresses IP, mais couvre 90% de 105 adresses IP soit 95 adresses IP. Le seuil des 90% ne peut plus être atteint par le seul AS1, et l'augmentation du nombre d'adresses IP dans le réseau a pour effet d'inclure l'AS2 dans les points de contrôle. **Lorsque l'augmentation du nombre d'adresses IP attribuées à un réseau national (ici 5) conduit à ce que le nombre d'AS nécessaires pour connecter 90% des adresses IP (95) devienne supérieur au nombre d'AS attribuées aux points de contrôle existants (90), on assistera mécaniquement à une hausse du nombre de points de contrôle.**

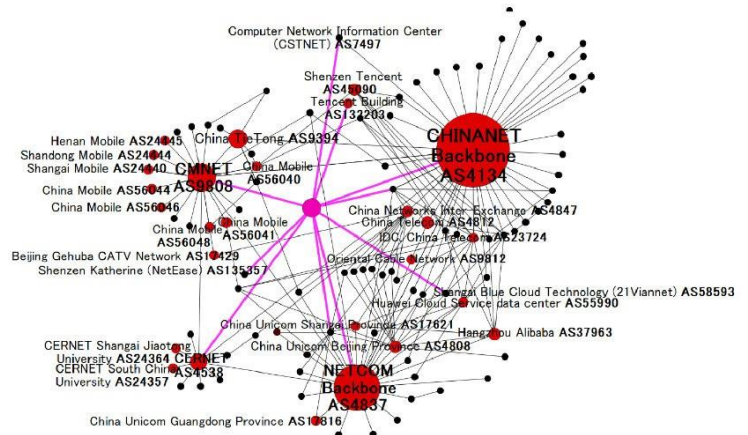
Par la démultiplication des points de contrôle, tout réseau IP se décentralise donc automatiquement à mesure que s'accroît le nombre d'adresses IP attribuées à un réseau d'acheminement. Cette décentralisation automatique du réseau par l'augmentation du nombre d'adresses IP est néanmoins contrecarrée dans deux situations : lorsque les adresses IP nouvellement attribuées (depuis 2011 ici) le sont principalement voire exclusivement par l'un des points de contrôle antérieurs (de 2011 ici), auquel cas l'augmentation du nombre d'adresses IP équivaut au nombre d'adresses IP attribuées par les points de contrôle antérieurs et ne laisse donc apparaître aucun nouveau point de contrôle ; ou lorsque l'augmentation du nombre d'adresses IP profite à de nouveaux AS et donc à de nouveaux points de contrôle, mais que ces AS et points de contrôle appartiennent aux opérateurs propriétaires des points de contrôle antérieurs, auquel cas l'augmentation du nombre de points de contrôle ne s'accompagne pas d'une diversification des gestionnaires. Dans ces deux cas, les gestionnaires des points de contrôle antérieurs maintiennent leur domination malgré la hausse du nombre d'adresses IP. On a utilisé le logiciel Gephi de modélisation d'un réseau pour représenter ainsi la centralisation des réseaux nationaux d'acheminement comparés à partir des 100 plus gros AS constituant chacun de ces réseaux en 2022 :

⁹⁴⁰ On l'observe fortement en Chine, où les petits AS (attribuant moins de 2048 adresses IP) enregistrés depuis 2011 sont souvent des AS qui connectent des serveurs *cloud* – par exemple l'AS136600 Fengniao Cloud (768 adresses IP) enregistré en 2020, les AS137801 AIPO Cloud (1024 adresses IP), AS137787 CACloud Services (1024 adresses IP), AS7586 Cloudfort IT (1536 adresses IP) et AS56011 Unicloud Tech (516 adresses IP) enregistrés en 2021

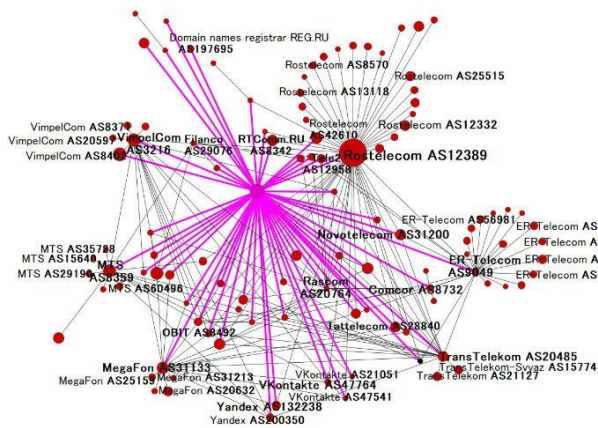
Réseau français des 100 plus gros AS



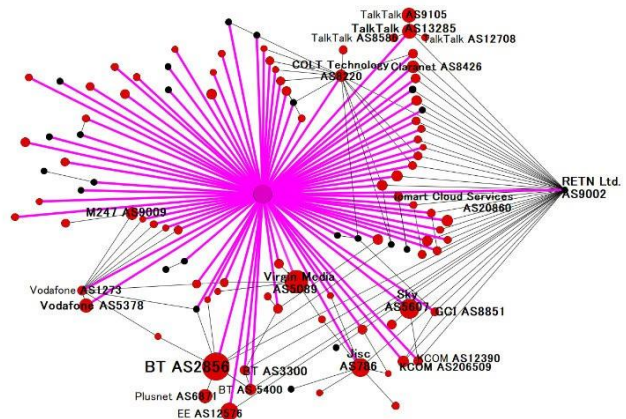
Réseau chinois des 100 plus gros AS



Réseau russe des 100 plus gros AS



Réseau britannique des 100 plus gros AS



Dans ces modélisations, chaque nœud représente un AS, dont la taille varie proportionnellement au nombre d'adresses IP qu'il connecte dans le réseau national. Les nœuds de couleur rouge représentent les points de contrôle. On a disposé en cercle – ou en triangle si le nombre de points concernés ne le permettait pas – et en bordure du réseau les AS qui appartiennent à un même opérateur. En Chine, parmi les 100 premiers AS, on observe ainsi quatre cercles principaux (China Telecom qui gère CHINANET, China Unicom qui gère Netcom, China Mobile et le réseau interuniversitaire CERNET), complétés par trois autres grands opérateurs (Tencent au nord, Huawei et Alibaba au sud-est sur les schémas). En France, on relève principalement un cercle (Renater) et trois triangles (Orange, SFR et Free) complétés par deux autres grands opérateurs (OVH et Bouygues). En Russie, on relève au moins cinq cercles (Rostelecom, ER-Telecom, Vimpelcom, Mobile TeleSystems dit MTS et MegaFon), deux triangles (TransTelekom dit TTK et VKontakte, qui gère aussi le premier réseau social russe, équivalent à Facebook) et plusieurs autres grands opérateurs (Yandex qui gère aussi le moteur de recherche russe, Moscow Telecommunications Corporation aussi dit ComCor, Filanco, Novotelecom, Rascom...). Au Royaume-Uni, on identifie un cercle formé au sud par BT et ses

filiales (Plusnet et EE), un triangle formé au nord-est par TalkTalk et plusieurs autres grands opérateurs (Virgin, Sky, Vodafone, iomart, Colt Technology Services, GCI, M247, KCOM, Jisc⁹⁴¹ ...).

Les liens entre les nœuds représentent les relations de peering entre les différents AS, *i.e.* celles de leurs interconnexions qui créent des points d'échange (ou IXP, Internet Exchange Points) entre les AS⁹⁴². Ces points d'échange sont donc ici symbolisés par des liens. Les liens de couleur violette représentent les points d'échange entre un AS présent dans le réseau national et un AS présent dans un réseau étranger. Le nœud violet représente quant à lui tout AS étranger. En cartographiant ainsi la structure de chaque réseau national d'acheminement, ces schémas permettent donc : d'identifier les points de contrôle parmi les 100 plus gros AS d'un réseau national d'acheminement ; de visualiser la diversité des opérateurs gestionnaires de ces AS dans le réseau national ; de connaître les liens d'échange entre ces AS au sein du réseau national ; et d'observer les connexions entre les AS constitutifs d'un réseau national avec les AS constitutifs d'un réseau étranger.

Ces schémas laissent d'ores et déjà apercevoir plusieurs caractéristiques de nos quatre réseaux nationaux d'acheminement. En Chine, la majorité des 100 plus gros AS appartient à quatre opérateurs (4 opérateurs différents se partagent 66 des 100 plus gros AS), et seuls 10 AS sont directement connectés à un réseau étranger dont 8 sont des points de contrôle. Ces traits laissent présager, dans le réseau chinois, un acheminement centralisé autour d'une faible diversité des opérateurs gérant les principaux AS, mais aussi une très faible diversité des voies d'accès au réseau international. En France, les principaux points de contrôle appartiennent sept opérateurs mais surtout, la majorité des 100 plus gros AS appartient à une multitude d'opérateurs (65 des 100 plus gros AS sont détenus par 65 opérateurs différents), et 53 AS sont directement à un réseau étranger dont 13 sont des points de contrôle.

On observe que l'augmentation du nombre de points de contrôle en France et en Chine depuis 2011 a eu un effet décentralisateur très différent dans les deux réseaux. En Chine, sur les 24 nouveaux points de contrôle depuis 2011, 6 d'entre eux reviennent à cinq opérateurs chinois (Oriental Cable, Tencent, Alibaba, Huawei et Beijing Gehua CATV), trois d'entre reviennent au ministère de l'Éducation (réseau CERNET qui n'était pas un point de contrôle en 2011) et 15 d'entre eux reviennent aux trois points de contrôle de 2011. Cela signifie que les trois opérateurs (China Telecom, China Unicom et China Mobile) gestionnaires des points de contrôle existants en 2011 ont maintenu leur domination sur la majorité des nouveaux points de contrôle, et que les nouveaux gestionnaires des points de contrôle sont peu diversifiés (6 nouveaux gestionnaires de points de contrôle). En France, sur les 22 nouveaux points de contrôle depuis 2011, l'un d'entre eux revient à un établissement public à caractère industriel et commercial (le Commissariat à l'énergie atomique et aux énergies alternatives, organisme de recherche dans les domaines de l'énergie, de la défense, des technologies

⁹⁴¹ Jisc est une société à but non lucratif qui interconnecte des établissements universitaires, publics ou à but non lucratif. Elle est issue de lettres d'orientation du 1^{er} avril 1993 des Secrétaires d'État des Conseils de financement de l'enseignement supérieur d'Angleterre, d'Écosse et du pays de Galles, invitant lesdits Conseils à créer un comité mixte gérant spécialement la mise en réseau de l'enseignement supérieur.

⁹⁴² On a vu que d'autres types d'interconnexions existent entre opérateurs, tels que le transit IP qui n'établit pas de point d'échange entre deux AS mais par lequel un opérateur loue à un autre une partie des fréquences hertziennes qu'il a lui-même obtenues auprès des autorités de régulation des radiofréquences (Arcep et Autorité nationale des fréquences en France, Ofcom au Royaume-Uni, Roskomnadzor en Russie, et la State Radio Regulation of China (SRRC) en Chine placée sous l'autorité du ministre de l'Industrie et des Technologies de l'information)

de l'information et de la communication, des sciences de la matière, de la vie et de la santé) et un autre revient à un opérateur étranger (Norsk Hydro, norvégien), 3 points de contrôle reviennent à des opérateurs régionaux (Moselle Telecom, Teloise, Iris 64 dans les Pyrénées-Atlantiques), 2 reviennent à des banques françaises (Crédit Agricole et BNP Paribas), 3 reviennent à des opérateurs français tier 2 (Wilfirst, Céleste, Sewan) et 12 reviennent aux sept points de contrôle de 2011. Cela signifie que les six opérateurs (Orange, SFR, Free, Bouygues, OVH, Renater) gestionnaires des points de contrôle existants en 2011 ont maintenu leur domination sur la moitié des nouveaux points de contrôle, mais que les nouveaux gestionnaires des points de contrôle sont relativement diversifiés (10 nouveaux gestionnaires). En France, l'augmentation du nombre de points de contrôle a eu un effet plus décentralisateur qu'en Chine du côté des nouveaux gestionnaires (10 en France contre 6 en Chine), mais les gestionnaires des points de contrôle de 2011 ont maintenu leur domination dans les deux réseaux en s'appropriant les plus gros AS (en nombre d'adresses IP attribuées).

Sur le plan des techniques de régulation, la disposition des AS en cercle dans un réseau d'acheminement (*i.e.* l'appropriation par un même opérateur d'une multitude d'AS) permet d'instaurer un réseau en étoile à l'intérieur du réseau maillé internet. En laissant entrevoir 4 principaux réseaux en étoile, la cartographie des 100 premiers AS du réseau chinois révèle une forte centralisation des principaux AS, et donc de l'essentiel de l'acheminement chinois. Si la carte faisait apparaître un seul réseau en étoile auquel tous les AS étaient liés, l'acheminement serait extrêmement centralisé par son gestionnaire. Inversement, si la carte fait apparaître une multitude d'étoiles, l'effet centralisateur de cette structure sera moindre car les gestionnaires des étoiles seront plus diversifiés. C'est le cas en Russie, où l'on compte au moins huit étoiles annoncées par les 100 premiers AS (Rostelecom, ER-Telecom, Vimpelcom, Mobile TeleSystems, MegaFon, VKontakte, TTK et Yandex), et où par ailleurs un grand nombre des 767 points de contrôle de la carte ne relève d'aucune de ces étoiles. Le réseau russe mélange une pluralité d'étoiles avec un réseau maillé géré par une multitude d'opérateurs tier 2 (tel que Ru-Center, Perviy, Delta Telecom Ltd, Kvant Telecom, Severen-Telecom, l'hébergeur Rusonyx...). Au surplus, chaque AS est relié à un grand nombre d'autres AS, suggérant ainsi que la connexion de chaque AS au réseau national dépend d'une pluralité d'opérateurs tiers et non d'un seul opérateur tiers. La connexion de 90% du réseau d'acheminement russe repose donc sur une forte interdépendance d'un très grand nombre d'AS aux gestionnaires très diversifiés, ce qui traduit un acheminement particulièrement décentralisé en Russie.

Quant au Royaume-Uni, la carte du réseau des 100 plus gros AS illustre elle aussi une forte décentralisation, dont les causes sont toutefois très différentes voire, pour certaines, contraires à celles de la décentralisation du réseau russe : la petite taille des réseaux en étoile (BT et TalkTalk) et leur très faible nombre (2) signalent une grande diversité des opérateurs ; et les AS constitutifs du réseau national sont moins reliés entre eux, faisant ainsi reposer la connexion de 90% du réseau national non pas sur une forte interdépendance des AS mais au contraire sur une forte indépendance de chaque AS vis-à-vis des autres. Les cartes russe et britannique proposent donc deux structures variées de réseaux très décentralisés d'AS.

Sur un plan juridique, ces différentes cartes font voir les conséquences de plusieurs réglementations décrites jusqu'à présent. La décentralisation de l'acheminement constatée sur la carte du réseau russe confirme l'ouverture du marché de la fourniture d'accès internet par la loi de 1996 sur les médias de masse, et l'exploitation de cette ouverture par des opérateurs de différentes régions peu voire non couvertes en raison de leurs conditions géographiques. En Chine, par le faible nombre de liens avec des AS étrangers, la carte retranscrit le peu

d'autorisations délivrées par le Bureau d'entrée et de sortie des communications internationales (ministère de l'Industrie et des Technologies de l'information) depuis la promulgation par le Conseil des affaires de l'État des dispositions provisoires pour la gestion de la connexion internationale des réseaux informatiques en 1996. Au Royaume-Uni, où l'Ofcom priorise la liberté du consommateur de choisir son opérateur dans le cadre du principe de neutralité d'internet, la carte du réseau national d'AS retranscrit des opérateurs très indépendants les uns des autres et hautement connectés au réseau international. Pour chacun de ces réseaux, les réglementations étatiques semblent donc avoir effectivement orienté la structure des réseaux d'acheminement.

2. Conclusions sur la centralisation des réseaux nationaux d'acheminement

Pour évaluer et comparer la centralisation de l'acheminement dans ces réseaux nationaux, on s'appuie sur trois critères : la connexion des adresses IP dans le réseau national (afin de mesurer la centralisation des accès nationaux dans le réseau) ; la connexion des AS au réseau international (afin de mesurer la centralisation des accès internationaux dans le réseau) ; et l'étatisation des accès nationaux et internationaux dans le réseau. On apprécie la centralisation de la connexion des adresses IP dans le réseau national selon quatre paramètres : le nombre de points de contrôle ; la proportion d'AS qui se partagent les points de contrôle parmi la totalité des AS auxquels sont attribués des adresses IP dans le réseau national (valeur de contrôle) ; le nombre d'opérateurs propriétaires et donc gestionnaires des points de contrôle (diversité des gestionnaires des points de contrôle) ; et le nombre d'opérateurs propriétaires des 100 plus gros AS (diversité des gestionnaires des principaux AS). On apprécie la centralisation de la connexion des AS au réseau international selon deux paramètres : le nombre d'AS directement connectés au réseau international parmi les 100 plus gros AS (diversité des principaux AS directement connectés au réseau international) ; et le nombre de points de contrôle directement connectés au réseau international (diversité des points de contrôle directement connectés au réseau international).

On prend en compte une dernière variable qu'on appellera « AS auxiliaires ». Par AS auxiliaires, on entend tout AS membre du réseau national hors points de contrôle. Sur les cartes, les AS auxiliaires présents parmi les 100 plus gros AS sont les nœuds de couleur noire. La notion d'AS auxiliaires permet d'évaluer le rapport entre les points de contrôle et les autres AS constitutifs du réseau national, et notamment le rapport de dépendance des premiers au seconds. Un AS auxiliaire se connecte au réseau national indépendamment de tout point de contrôle s'il est membre de ce réseau en n'étant relié par *peering* à aucun point de contrôle ; de même, il se connecte au réseau international indépendamment de tout point de contrôle s'il est directement relié par *peering* à un AS étranger. Une indépendance des AS auxiliaires pour se connecter aux réseaux national et international traduit une diversification des voies de communication au-delà de celles maîtrisées par les points de contrôle. Inversement, un AS dépend d'un point de contrôle pour se connecter au réseau national s'il est relié par *peering* à ce point de contrôle ; de même, il ne peut accéder indépendamment au réseau international s'il n'est relié par *peering* à aucun AS étranger. Une dépendance des AS auxiliaires pour se connecter aux réseaux national et international traduit un resserrement des voies de communications autour de celles maîtrisées par les points de contrôle. Par conséquent, l'indépendance des AS auxiliaires donne la possibilité de connaître l'écho, l'influence des points de contrôle auprès des autres AS constitutifs du réseau national : les 10% d'adresses IP que les AS auxiliaires connectent au réseau peuvent servir à renforcer la centralité des points de contrôle, ou au contraire à décentraliser la connexion de ces 10% d'adresses IP loin de ces points de contrôle.

Nous n'avons malheureusement pas pu examiner la totalité des AS auxiliaires pour chacun des réseaux nationaux comparés. On a cependant étudié un échantillon des 100 plus gros AS auxiliaires afin d'observer certaines tendances. Par exemple, en France où on dénombre 29 points de contrôle, notre échantillon inclut tous les AS compris entre le 30^e plus gros AS et le 130^e plus gros AS par le nombre d'adresses IP connectées. En Russie, notre échantillon inclut tous les AS compris entre le 768^e et le 868^e plus gros AS et ainsi de suite. Pour chacun des réseaux comparés, on note d'abord la proportion d'AS auxiliaires, parmi les 100 plus gros AS auxiliaires, qui sont reliés à des points de contrôle : plus ce pourcentage est élevé, plus les gros AS auxiliaires dépendent des points de contrôle pour se connecter au réseau national, plus les AS auxiliaires centralisent les voies d'accès nationales. On relève par ailleurs la proportion d'AS auxiliaires, parmi les 100 plus gros, qui sont directement reliés à des AS étrangers : plus ce pourcentage est élevé, moins les gros AS auxiliaires dépendent des points de contrôle pour se connecter au réseau international, plus les AS auxiliaires décentralisent les voies d'accès internationales.

Critère de centralisation de l'acheminement	Paramètre de centralisation de l'acheminement	FR	CN	RU	UK
Connexion des adresses IP dans le réseau national (centralisation des accès nationaux)	Nombre de points de contrôle	29	27	767	82
	Proportion d'AS se partageant les points de contrôle (valeur de contrôle)	1.8%	4.74%	15.39%	4.21%
	Nombre d'opérateurs propriétaires des points de contrôle	16	9	595	74
	Nombre d'opérateurs propriétaires des 100 premiers AS	66	31	48	89
	Proportion d'AS auxiliaires connectés à des points de contrôle parmi les 100 plus gros AS auxiliaires	57%	99%	97%	50%
Connexion du réseau national au réseau international (centralisation des accès internationaux)	Parmi les 100 premiers, nombre d'AS directement connectés au réseau international	53	10	51	83
	Nombre de points de contrôle directement connectés au réseau international	13	5	317	69
	Proportion d'AS auxiliaires directement connectés au réseau international parmi les 100 plus gros AS auxiliaires	60%	8%	45%	66%
Centralisation de la connexion des adresses IP et au réseau international par l'État	Nombre de points de contrôle dont l'État est propriétaire	4/29	21/27	76/767	4/82
	Nombre d'opérateurs dont l'État est propriétaire parmi les points de contrôle	2/16	4/9	16/595	5/74
	Parmi les 100 premiers, nombre d'AS directement connectés au réseau international dont l'État est propriétaire	1/52	7/10	2/51	1/89
	Nombre de points de contrôle directement connectés au réseau international dont l'État est propriétaire	1/13	4/5	10/317	1/69

Comme pour les tableaux précédents, on a entouré en bleu foncé les réseaux les plus centralisés et en bleu clair les réseaux les plus décentralisés selon tel ou tel paramètre. La Chine est de loin le réseau d'acheminement le plus centralisé, tant pour les accès nationaux qu'internationaux, concernant 11 des 12 paramètres retenus. Aussi, on observe en premier lieu que **la Chine et la Russie s'opposent radicalement sur leurs réseaux sous-marin et d'acheminement respectifs** : le réseau sous-marin russe est le plus décentralisé de ceux étudiés tandis que le réseau sous-marin chinois est assez décentralisé ; le réseau d'acheminement chinois est le plus centralisé de ceux étudiés tandis que le réseau d'acheminement russe dont les voies de communication nationales sont les plus décentralisées. En Chine, les voies de communication nationales sont centralisées dès l'acheminement, avant que le trafic parvienne aux câbles sous-marins décentralisés ; en Russie, les voies de communications sont centralisées dès le transport sous-marin, après que le trafic ait été acheminé de manière décentralisée⁹⁴³.

Ensuite, les chiffres relevés informent sur le fonctionnement propre à chacun des quatre réseaux nationaux d'acheminement. Ainsi en Chine, pour se connecter au réseau national, 99% des 100 plus gros AS auxiliaires dépendent de 27 points de contrôle gérés par 9 opérateurs ; de même seuls 8% de ces AS auxiliaires sont directement reliés à un AS étranger, en sorte que 92% des 100 plus gros AS auxiliaires dépendent des mêmes 27 points de contrôle pour se connecter au réseau international. En pratique, cela signifie que les AS autres que des points de contrôle peuvent très difficilement se connecter au réseau national ou international sans passer par un point de contrôle. Les points de contrôle semblent donc avoir un puissant écho centralisateur auprès des AS auxiliaires, dont la dépendance aux points de contrôle existants renforce la centralité de ces derniers à travers le réseau chinois de l'acheminement. L'accès au réseau international, tout comme les points de contrôle, sont par ailleurs fortement étatisés en Chine : actionnaire majoritaire de China Telecom, China Unicom et China Mobile et gestionnaire direct de CERNET, l'État est propriétaire de 21 des 27 points de contrôle soit 77.77% de la totalité des points de contrôle et possède par ailleurs 4/5 soit 80% de la totalité des points de contrôle connectés au réseau international. Ces chiffres et cette carte rendent compte d'un **réseau chinois de l'acheminement dont les AS qui le constituent dépendent remarquablement de points de contrôle gérés par des opérateurs peu diversifiés pour pouvoir se connecter à des voies d'accès largement dominées par l'État, que ces voies d'accès au réseau soient nationales ou internationales**.

En France, 57% des plus gros AS auxiliaires dépendent de 30 points de contrôle gérés par 16 opérateurs. Cela signifie qu'un peu plus de la moitié des AS autres que des points de contrôle se connecte au réseau national en passant par des points de contrôle. En d'autres termes, la possibilité de se connecter au réseau national sans passer par un point de contrôle est ouverte pour les AS auxiliaires (cette possibilité est exploitée par un peu moins de la moitié de ceux échantillonnés) mais les points de contrôle existants maintiennent leur domination pour la connexion des AS au réseau national. Cela confirme l'observation déjà faite selon laquelle les nouveaux gestionnaires des points de contrôle depuis 2011 se sont pluralisés (11 nouveaux gestionnaires) bien que la moitié des nouveaux points de contrôle ait bénéficié aux points de contrôle existants en 2011. Le réseau français de l'acheminement semble donc suivre une tendance très lente et

⁹⁴³ La centralisation russe s'est d'ailleurs peut-être reportée sur le réseau sous-marin compte tenu des difficultés économiques et organisationnelles à centraliser un réseau national d'acheminement très diversement géré selon les caractéristiques propres à chaque environnement géographique régional (Sakhaline, Sibérie, Oural, Saint-Pétersbourg, région extrême-orientale...)

progressive de diversification de ses voies d'accès nationales. Cette tendance ne masque pas une certaine centralisation des voies d'accès nationales par la diversité encore très relative des gestionnaires de points de contrôle (16) et surtout par la très faible proportion d'AS détenteurs des points de contrôle (1.8% parmi tous les AS constitutifs du réseau national, faisant du réseau français de l'acheminement le réseau le plus centralisé selon le paramètre de la valeur de contrôle). Le maintien de la domination des points de contrôle par les 7 opérateurs de 2011 conjugué avec la concentration des points de contrôle par un petit pourcentage d'AS à l'échelle du réseau gérés par des opérateurs relativement diversifiés révèlent un réseau dont les voies d'accès nationales sont assez peu décentralisées.

Au contraire, les voies d'accès internationales sont quant à elles assez diversifiées : 53 des 100 plus gros AS et 60% des 100 plus gros AS auxiliaires sont directement connectés à des AS étrangers. En pratique, cela signifie que la majorité des AS auxiliaires ne dépend d'aucun point de contrôle pour se connecter au réseau international (tandis que la majorité des AS auxiliaires dépendent d'un point de contrôle pour se connecter au réseau national), et que la majorité des AS offrent chacun une voie internationale d'accès. Enfin, quoique plus importante qu'au Royaume-Uni, la centralisation étatique est très relative, concernant les voies d'accès tant nationales qu'internationales. L'État ne possède que 4/29 soit 13.79% des points de contrôle, dont trois d'entre eux sont gérés par Orange sur lequel l'État n'a qu'un pouvoir très minimal de décision comme on l'a vu, et dont le dernier géré par un établissement public à caractère industriel et commercial (Commissariat à l'énergie atomique et aux énergies renouvelables) n'est emprunté qu'à des fins scientifiques et universitaires et non à des fins civiles ou professionnelles. En sus, l'État ne possède via Orange que 1/13 soit 7.69% des points de contrôle connectés au réseau international et 1/52 soit 1.92% des 52 plus gros AS connectés au réseau international.

Ces constats correspondent à peu près avec celui fait pour le réseau sous-marin français – dont les voies nationales d'accès sont moins diversifiées par le nombre de câbles et plus étatisées quoique plus diversement gérées qu'au Royaume-Uni et aux États-Unis, mais dont les voies internationales d'accès sont les plus diversifiées par le nombre de pays étrangers que dessert le réseau sous-marin français. En somme, ces chiffres et cette carte rendent compte d'un **réseau français de l'acheminement à la fois peu décentralisé par ses voies nationales d'accès** (maintien de leur domination par les points de contrôle de 2011, très faible proportion d'AS gestionnaires de points de contrôle, dépendance d'un peu plus de la moitié des 100 plus gros AS auxiliaires aux points de contrôle...) **mais en cours de décentralisation** à un rythme très lent (diversité des nouveaux gestionnaires de points de contrôle, diversité des opérateurs gestionnaires de 100 plus gros AS, indépendance d'un peu moins de la moitié des AS auxiliaires à l'égard des points de contrôle, étatisation très relative et de plus en plus relative des points de contrôle...), **et décentralisé par ses voies internationales d'accès** (indépendance de la majorité des AS auxiliaires à l'égard des points de contrôle pour se connecter à un réseau étranger, majorité des 100 plus gros AS directement connectée au réseau international, diversité des points de contrôle fournissant une voie internationale d'accès...).

En Russie, les voies nationales d'accès sont hautement décentralisées par le nombre de points de contrôle, par la diversité des opérateurs gestionnaires des points de contrôle et par la proportion d'AS gestionnaires de points de contrôle parmi les 4 982 AS qui se voient attribués des adresses IP dans le réseau national. Le pourcentage élevé d'AS auxiliaires dépendants de points de contrôle s'explique par la très grande quantité de points de contrôle : une dépendance de 97% des 100 plus gros AS auxiliaires à 767 points de contrôle gérés par 578 opérateurs privés différents est très loin d'égaliser la dépendance de 99% des AS auxiliaires à 27 points de contrôle en Chine dont 21 appartiennent à l'État. L'accès au réseau international est aussi très

décentralisé en Russie, avec des points de contrôle qui proposent 317 voies d'accès à un réseau étranger. Plus encore, au-delà même des points de contrôle, 45% des 100 plus gros AS auxiliaires sont directement reliés au réseau international sans devoir emprunter un point de contrôle pour ce faire. L'étatisation du réseau d'acheminement est faible par rapport au nombre de points de contrôle : la Fédération détient 76/767 soit 9.9% des points de contrôle. 21 de ces points de contrôle appartiennent totalement à l'État (généralement des universités, laboratoires de recherche, services budgétaires ou militaires...⁹⁴⁴) et les 55 autres lui appartiennent partiellement via Rostelecom. Parmi les quatre réseaux nationaux d'acheminement comparés, le réseau russe est même le moins étatisé par la proportion d'opérateurs qui gèrent des points de contrôle et dont l'État est propriétaire – l'État ne possède que 16/595 soit 2.68% des opérateurs qui gèrent des points de contrôle. En somme, ces chiffres et cette carte rendent compte d'un **réseau russe de l'acheminement** dans lequel les **voies d'accès tant nationales qu'internationales sont très décentralisées, un réseau dominé par des opérateurs privés, grandement diversifiés, très interdépendants pour connecter l'essentiel des adresses IP au réseau national, indépendants les uns des autres pour connecter ces adresses IP au réseau international, et répartissant 90% des adresses IP du réseau entre des voies internationales d'accès notablement diverses.**

Enfin, par rapport aux trois autres réseaux, la décentralisation au Royaume-Uni bat des records sur quatre terrains : la diversité des opérateurs parmi les 100 plus gros AS (74) ; l'indépendance des 100 plus gros AS auxiliaires à l'égard des points de contrôle pour se connecter au réseau tant national (50% de dépendance) qu'international (34% de dépendance) ; la proportion de connexions directes au réseau international par les 100 plus gros AS (83%) et par les AS auxiliaires (66%) ; et la minimisation de toute appropriation des AS par l'État. En effet, sur les 82 points de contrôle, l'État n'en possède que quatre⁹⁴⁵ et domine encore moins de voies de communication internationales (1 voie appartenant à l'État sur 69 autres voies internationales fournies par les points de contrôle, 1 sur les 89 fournies par les 100 plus gros AS). Ces chiffres et cette carte rendent compte d'un **réseau britannique de l'acheminement nettement décentralisé, tant par le nombre des points de contrôle que par l'indépendance des AS auxiliaires à l'égard des points de contrôle** (à la différence de la Russie dont les AS auxiliaires dépendent des points de contrôle pour se connecter au réseau national), **tant par la diversité des voies nationales que par celle des voies internationales d'accès, tant par la diversité des opérateurs que par l'étatisation minimale du réseau.**

⁹⁴⁴ Parmi les 595 FAI gestionnaires des points de contrôle, les 15 FAI appartenant totalement à l'État sont : l'Institut fédéral de recherche scientifique pour l'analyse des systèmes de l'Académie des sciences de Russie ; l'Institut commun de recherche nucléaire ; l'Institut Kourtchatov Centre scientifique russe ; l'Institution budgétaire fédérale d'État pour l'Éducation et l'Enseignement Supérieur – Université d'État Lomonossov de Moscou ; l'Université d'État de Saint Pétersbourg ; l'Université polytechnique nationale de recherche de Tomsk ; la Coopérative de production – Laboratoire économico-juridique ; le Centre fédéral de recherche en technologies de l'information ; l'Institution budgétaire fédérale d'État pour les sciences – Institut de recherche spatiale de l'Académie russe des sciences ; l'Institut de physique générale de l'Académie russe des sciences ; l'Institution budgétaire fédérale d'État pour l'Éducation et l'Enseignement Supérieur – Université d'État du Kouban ; l'Établissement fédéral d'État d'enseignement supérieur autonome – Université d'État de Perm ; l'Institut de mathématiques et de mécanique du département de l'Oural de l'Académie russe des sciences ; l'Université technique d'État de Moscou-Bauman ; l'Université d'État en technologie de l'information, mécanique et optique (ITMO) de Saint-Pétersbourg ; et le Service de la Garde fédérale russe

⁹⁴⁵ L'AS198864 du Queen Mary and Westfield College University of London, l'AS7 du Laboratoire des sciences et des technologies de la Défense, l'AS201773 de l'Université de Warwick, et l'AS39400 du Quartier londonien de Hackney

En conclusion, nos résultats nous permettent de comparer les centralisations d'initiative étatique avec celles d'initiative privée. On a vu que le réseau sous-marin russe, centralisé principalement à l'initiative de l'État, est de loin le réseau sous-marin le plus centralisé parmi ceux comparés. On a vu aussi que le réseau chinois de l'acheminement, centralisé principalement à l'initiative de l'État, est de loin le plus centralisé parmi ceux comparés. L'observation la plus intéressante réside dans le fait que ces deux réseaux sont les plus centralisés sur la quasi-totalité des paramètres retenus *même en faisant abstraction des paramètres d'étatisation du réseau* (appropriation par l'État des opérateurs, des points de contrôle, des câbles sous-marins et de leurs gestionnaires, des voies d'accès internationales du réseau...). Autrement dit, même à supposer que les voies d'accès nationales et internationales du réseau fussent libérées de l'État, ces réseaux resteraient les plus centralisés parmi ceux comparés. Ainsi, dans tous les cas étudiés, le réseau national est plus centralisé lorsque la centralisation est d'initiative étatique et plus décentralisé lorsqu'elle est d'initiative privée. Cela ne signifie pas qu'une centralisation d'initiative publique est systématiquement plus centralisatrice qu'une centralisation d'initiative privée (par ex. un opérateur privé propriétaire de tous les points de contrôle et qui serait le seul à fournir un accès direct à un seul réseau étranger). Cela signifie en revanche que, dans chaque cas étudié, aussi bien pour les réseaux sous-marins que pour ceux d'acheminement, la centralisation d'initiative étatique accompagne un resserrement des voies d'accès tant nationales qu'internationales (y compris en Iran d'après les résultats relevés plus haut), tandis que les initiatives privées accompagnent au contraire une diversification des voies d'accès tant nationales qu'internationales voire une forte décentralisation de ces voies d'accès.

D) L'internet le plus centralisé au monde : le cas de la Corée du Nord

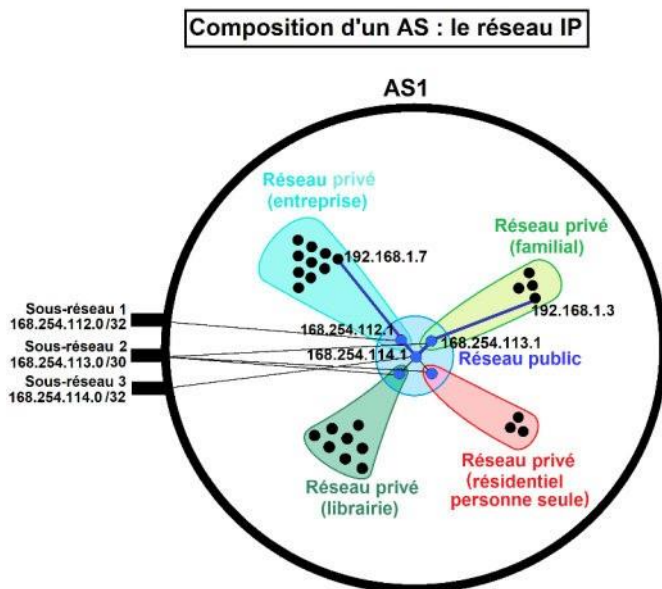
1. La connexion du réseau IP

On étudie enfin le cas extraordinaire du réseau nord-coréen d'acheminement. La compréhension des techniques de régulation d'internet employées par l'État nord-coréen nécessite quelques bases sur le fonctionnement d'un AS. L'exploitant d'un AS, *i.e.* un opérateur, se voit attribuer à sa demande un ensemble d'adresses IP de la part du registre Internet régional de sa région – un acteur privé à but non lucratif mandaté par l'Icann pour attribuer les adresses IP dites « publiques » aux AS dans les régions du monde⁹⁴⁶. Par le biais d'un de ses registres Internet régionaux, l'Icann peut par exemple octroyer 4096 adresses IP publiques à un AS. Une fois les adresses IP obtenues, l'exploitant de l'AS les réattribue à ses routeurs passerelles (box, modem... présents dans les locaux des abonnés) et à ses routeurs IP (présents dans ses locaux ou ceux d'un centre de données). L'ensemble des adresses IP publiques attribuées à ses routeurs par l'AS forme son « réseau public ».

L'adresse IP publique d'une passerelle n'identifie pas seulement cette passerelle : elle identifie collectivement toutes les machines des abonnés qui sont directement connectées à cette passerelle – par ex., toutes les machines (smartphones, ordinateurs...) connectées à une même box possèdent la même adresse IP publique. Commune à toute machine qui s'y connecte directement, l'adresse IP publique d'une passerelle ne permet pas d'identifier individuellement chacune des machines qui s'y connecte. Pour les distinguer, la passerelle confère une adresse

⁹⁴⁶Il existe cinq registres Internet régionaux : le RIPE-NCC (Réseaux IP européen), l'APNIC (Asia Pacific Network Information Center), l'ARIN (American Registry for Internet Numbers), le LACNIC (Latin America and Caribbean Network Information Center) et l'AfriNIC (African Network Information Center)

IP privée différente à chacune des machines qui lui sont directement connectées. Les adresses IP privées attribuées par les routeurs de l'AS forment les différents « réseaux privés » constitutifs de cet AS.



Dans le schéma ci-contre, le grand cercle noir représente un AS fictif (AS1). Les nœuds bleus au cœur de l'AS représentent 5 adresses IP publiques attribuées par l'AS1. Quatre de ces cinq adresses publiques sont attribuées à des passerelles (nœuds bleu foncé), la cinquième (bleu clair) est attribuée à un routeur IP. Les nœuds noirs représentent les adresses IP privées connectées aux adresses publiques. En l'espèce, quatre réseaux privés sont connectés à quatre passerelles différentes. Deux adresses IP privées issues de deux réseaux privés différents peuvent communiquer via le réseau public en empruntant l'adresse publique de la passerelle à laquelle elles sont connectées.

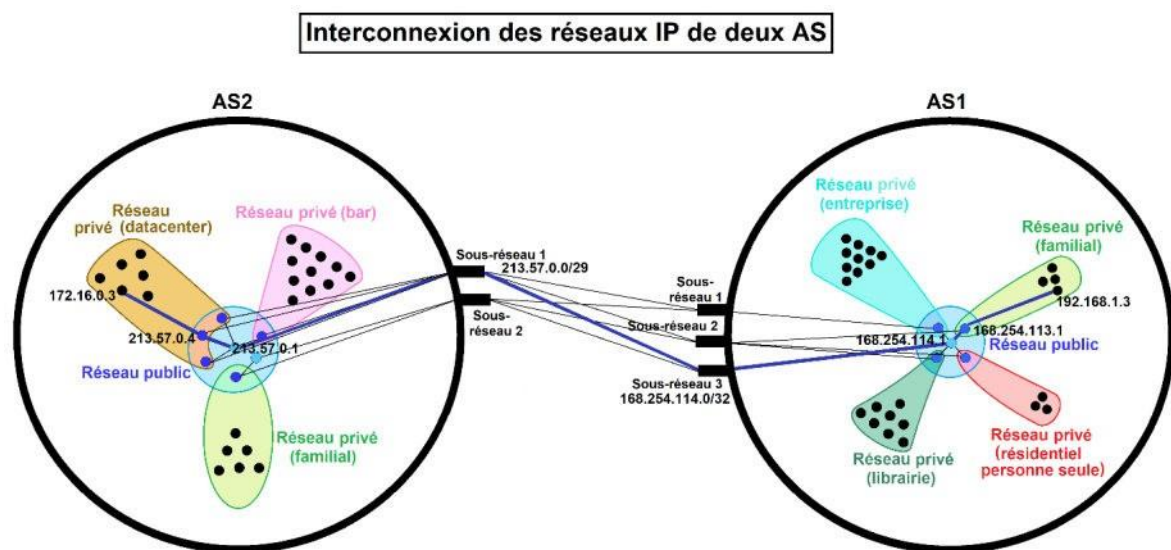
Par exemple, ci-contre (lien bleu), si un salarié membre du réseau d'entreprise souhaite communiquer avec une personne membre du réseau de la résidence familiale, le terminal de ce salarié (IP privée 192.168.1.7) devra emprunter l'adresse IP publique de la passerelle à laquelle il est directement connecté (IP publique 78.12.17.5). Ladite passerelle transmettra ensuite la requête à l'adresse publique du routeur IP (au centre), qui la retransmettra à son tour à la passerelle à laquelle est directement connecté le réseau familial (IP publique 10.9.2.2). Dès lors que la requête atteint la passerelle du réseau destinataire, cette passerelle n'a plus qu'à transmettre la requête au terminal définitivement destinataire de la requête (IP privée 192.168.1.3). Deux réseaux privés peuvent ainsi communiquer entre eux grâce à leurs adresses IP publiques respectives.

Les adresses IP publiques sont les points de connexion des réseaux privés avec le réseau public, et le réseau public et l'espace collectif de communication dans lequel circulent les requêtes provenant des différents réseaux privés. Le réseau public d'internet est formé par l'ensemble des adresses IP publiques, *i.e.* par l'ensemble des routeurs de tous les AS interconnectés dans le monde, y compris l'AS nord-coréen. On a ici représenté une adresse IP par réseau privé mais un même réseau privé peut posséder plusieurs adresses IP publiques, notamment s'il est très étendu (certains réseaux privés aéroportuaires, universitaires...), et rien n'interdit qu'un seul réseau privé possède toutes les adresses publiques attribuées par un AS. En revanche, deux réseaux privés distincts ne peuvent pas simultanément posséder les mêmes adresses IP publiques, et toute adresse IP publique est différente de toute autre adresse IP publique pour pouvoir se reconnaître mutuellement sur le réseau public international – raison pour laquelle les adresses IP sont mondialement gérées par un même acteur, l'Icann.

Ce schéma appelle une dernière explication : les sous-réseaux. Lorsque l'exploitant d'un AS reçoit les adresses IP publiques de la part de l'Icann, il peut les répartir en plusieurs sous-réseaux selon ses choix de gestion. Par exemple, sur le schéma, l'exploitant de l'AS1 répartit

les cinq adresses IP publiques en trois sous-réseaux de l'AS : le sous-réseau 1 couvre l'adresse publique du réseau d'entreprise ; le sous-réseau 2 couvre les adresses publiques du réseau familial, du réseau d'une librairie, et du réseau d'une personne vivant seule ; le sous-réseau 3 couvre l'adresse publique du routeur IP. Chaque sous-réseau possède sa propre adresse IP publique, dont la syntaxe se conclut par le symbole « / » suivi d'un nombre. Ce nombre indique la quantité d'adresses IP publiques couvertes par le sous-réseau : /32 indique que le sous-réseau couvre une seule adresse IP publique, /31 indique qu'il en couvre 2, /17 indique qu'il en couvre 32 766, /1 indique qu'il en couvre 2 147 483 646.

L'adresse d'un sous-réseau d'un AS est une porte d'accès à cet AS. L'accès à l'adresse 168.254.112.0/32 offre l'accès au sous-réseau 1, donc à l'adresse IP publique couverte par ce sous-réseau (78.12.17.5), donc au réseau privé directement connecté à cette adresse IP publique (réseau privé d'entreprise). L'accès à l'adresse 168.254.113.0/30 offre l'accès au sous-réseau 2, donc aux trois adresses IP publiques couvertes par ce sous-réseau, donc aux réseaux privés directement connectés à ces adresses IP publique (réseaux privés familial, d'une personne vivant seule et d'une librairie). L'accès à l'adresse 168.254.114.0/32 offre l'accès au sous-réseau 3, donc à l'adresse IP publique couverte par ce sous-réseau (adresse publique du routeur IP). L'accès aux trois sous-réseaux offre l'accès à l'intégralité du réseau IP de l'AS. Les adresses de sous-réseaux sont alors les portes d'accès à un AS, qui donnent aux membres du réseau public de cet AS le pouvoir d'accéder aux membres du réseau public d'un autre AS.



L'AS2 attribue 7 adresses IP publiques – cinq à des passerelles (nœuds bleu foncé), deux à des routeurs IP (nœuds bleu clair). Ces adresses IP publiques connectent trois réseaux privés au réseau public : le réseau privé d'un bar ; un réseau privé familial ; et le réseau privé d'un centre de données (établissement accueillant des serveurs voire des routeurs d'un ou plusieurs services, d'un ou plusieurs opérateurs). Le réseau privé du datacenter possède trois adresses IP publiques. L'exploitant de l'AS2 a découpé ses adresses IP publiques en deux sous-réseaux : le sous-réseau 1 qui couvre les adresses IP publiques du bar, du centre de données et d'un routeur IP ; le sous-réseau 2 qui couvre les adresses IP publiques du foyer familial et d'un routeur IP.

Deux réseaux privés issus de deux AS différents peuvent communiquer par le biais des sous-réseaux de chaque AS. En l'espèce, on suit le parcours (lien bleu) d'un terminal membre du réseau familial de l'AS1 (IP privée 192.168.1.3) qui accède à un serveur membre du réseau de

datacenter de l'AS2 (IP privée 172.16.0.3). Le membre du réseau familial communique sa requête à l'adresse de sa passerelle (IP publique 168.254.113.1), laquelle passerelle transmet la requête à celui des routeurs IP auxquels elle est connectée qui est le plus proche de la destination (ici un seul routeur IP auquel est connecté la passerelle, IP publique 168.254.114.1). Le routeur IP utilise son sous-réseau d'appartenance (IP publique 168.254.114.0/32) pour accéder à l'AS2. Précisément, il accède à l'AS2 par la porte 213.57.0.0/29, *i.e.* par le sous-réseau de l'AS2 auquel appartient le routeur IP (IP publique 213.57.0.1) le plus proche de la destination. Ce routeur IP n'a plus qu'à transmettre la requête à la passerelle (IP publique 213.57.0.4) à laquelle est connecté le serveur destinataire pour que ce serveur reçoive la requête de la part de sa passerelle.

À nouveau, l'échelle des AS est ici très minimaliste, simplifiée pour la compréhension du réseau IP. Un AS qui attribue des adresses IP publiques en attribue au minimum 256, et non 5 ou 7. Il faut alors compter au moins 256 nœuds bleus dans un AS de taille réelle. On a vu par exemple que le plus gros AS français – l'AS3215 exploité par Orange – attribue 20 111 104 adresses IP publiques. Cela signifie que, **sur ce seul AS, Orange contrôle l'accès à tous les réseaux privés connectés par ces plus de 20 millions d'adresses IP publiques** : il est capable de restreindre l'accessibilité (par blocage, filtrage, ralentissement...) de n'importe quel réseau privé qu'il interconnecte. On a vu néanmoins que le réseau IP français ne se limite pas à ce seul AS, et par ailleurs chaque AS engendre un réseau IP différent (selon le nombre d'adresses publiques qu'il attribue, le nombre et le type de réseaux privés qu'il connecte, les choix de répartition des adresses IP publiques en sous-réseaux...). **Un réseau IP national comprend tous les réseaux IP interconnectés par tous les AS constitutifs du réseau national de l'acheminement**, *i.e.* tous les réseaux privés interconnectés par les routeurs situés sur le territoire national. Ainsi, en France, le réseau IP national est formé par tous les réseaux privés et publics qu'interconnectent les 1276 AS qui attribuent des adresses IP publiques. Le périmètre du réseau IP national s'étend à 4982 AS en Russie, à 1948 AS au Royaume-Uni, 548 en Chine.

2. La centralisation étatique nord-coréenne du réseau IP

Le périmètre du réseau IP nord-coréen se limite à un seul AS répertorié par l'Asia Pacific Networks Information Centre⁹⁴⁷ : l'AS qui porte le numéro AS131279, intitulé « Ryugyong-dong ». Les routeurs constitutifs de cet AS sont gérés depuis 2009 par Star Joint Venture Co. (Star JV), entreprise publique et seul opérateur autorisé à attribuer des adresses IP publiques dans le pays⁹⁴⁸. Star JV est historiquement le premier opérateur à obtenir des adresses IP publiques de la part de l'Icann, ce qui signifie que **le réseau IP nord-coréen est né en 2009**. L'AS Ryugyong-dong est connecté par peering à deux AS étrangers : l'AS20485 de TTK en Russie et l'AS134544 de Cenbong Int'l Holdings Ltd (un opérateur sino-hong-kongais) à Hong-Kong⁹⁴⁹. Cela signifie que le réseau internet nord-coréen est connecté au réseau international par ces deux voies. Enfin, l'AS Ryugyong-dong ne possède que quatre adresses de sous-réseau :

947L'Asia Pacific Networks Information Centre (APNIC) est un Registre Internet régional, *i.e.* un organisme à but non lucratif auquel l'Icann délègue la mission d'attribuer les adresses IP publiques aux AS d'une région (ici l'Asie-Pacifique) et de tenir les registres publiquement consultables des adresses IP attribuées aux AS. Un AS ne peut obtenir des adresses publiques qu'en passant par un Registre Internet régional.

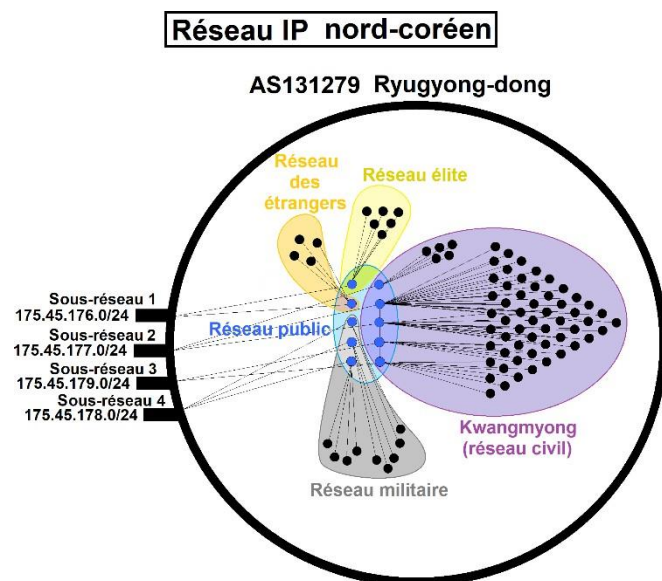
948WILLIAMS Martyn, « North Korea's Internet Domain Is in New Hands », sur *PCWorld.com*, 19 mai 2011. M. Williams est un journaliste britannique spécialisé depuis plus de quinze ans dans les technologies de réseau nord-coréennes.

949V. profil de l'AS131279 Ryugyong-dong sur *IPinfo.org*

175.45.176.0/24, 175.45.178.0/24, 175.45.179.0/24 et 175.45.177.0/24⁹⁵⁰. Ce sont là les quatre portes d'accès à l'internet nord-coréen, les quatre adresses IP nord-coréennes qui permettent aux machines membres de cet AS de communiquer avec les adresses IP de tous les autres AS mondialement connectés à internet. Par ailleurs, on a vu que la Corée du Nord coupe tout réseau sous-marin (par l'absence de câbles) et tout réseau hertzien (par un brouillage des ondes aux frontières). Dès lors, **l'internet nord-coréen tient tout entier dans un seul AS et ne possède que quatre portes d'accès**⁹⁵¹. Que sait-on de ce qu'il y a derrière ces portes ?

Tout d'abord, les adresses de sous-réseau indiquent, par la mention « /24 », que chaque sous-réseau couvre 256 adresses IP publiques. Cela signifie que **le réseau internet nord-coréen n'attribue que $256 \times 4 = 1024$ adresses IP publiques**. Par comparaison, on a vu que le réseau français en attribue 74 121 979 et que le réseau chinois en attribue 343 009 060. Cela signifie aussi que le nombre de voies d'accès au réseau IP public est extrêmement limité. Cette centralisation extrême des voies d'accès au réseau public suggère qu'un grand nombre d'adresses IP privées se partage un petit nombre d'adresses IP publiques⁹⁵². Elle implique aussi qu'il suffit à Star JV, et donc à l'État qui en est propriétaire, **de jouer sur un très petit nombre d'adresses IP publiques pour contrôler l'accessibilité de n'importe quel réseau privé membre de l'AS Ryugyong-dong, i.e. membre de l'internet nord-coréen**.

C'est très exactement ce que fait l'État en Corée du Nord. L'internet nord-coréen est constitué par des réseaux privés qui n'ont pas les mêmes droits d'accès à internet. On connaît au moins quatre types de réseaux privés en Corée du Nord : le réseau privé militaire ; le réseau privé civil (Kwangmyong, littéralement « Lumière ») ; le réseau privé des élites ; et le réseau privé des ambassades et ONG qui inclut aussi probablement les adresses IP privées des touristes. Dans le schéma ci-contre, on a représenté 10 des 1024 adresses IP publiques attribuées par l'AS Ryugyong-dong (nœuds bleus). On ignore comment la Corée du Nord répartit les adresses IP publiques dans ses sous-réseaux, et nous avons ici arbitrairement relié les adresses IP publiques à tel ou tel sous-réseau.



⁹⁵⁰Les trois premières ont été annoncées officiellement en juillet 2022 et enregistrées par la base de données *IPinfo.io*, qui agrège notamment la base de données de l'APNIC. Régulièrement actualisée, *IPinfo* a publié pour la première fois l'existence de cet AS le 14 juil. 2022. La 4^e, non officielle, est référencée par la base de données WHOIS de l'APNIC [en ligne].

⁹⁵¹Sans compter les portes d'accès satellitaires, dont on a évoqué celle qui connecte Berlin à la Corée du Nord

⁹⁵²En 2017, plus de 3.8 millions de nord-coréens étaient équipés de smartphones, qui semblent le moyen privilégié par les nord-coréens pour accéder à internet (KIM Jaewon, « North Koreans tap into smartphone apps on restricted state network » [en ligne], *Nikkei*, 6 juin 2019). En y ajoutant les ordinateurs ou encore les machines constituant le réseau militaire nord-coréen, il y a probablement une à plusieurs dizaines de millions d'adresses IP privées connectées à seulement 1024 adresses IP publiques.

Cependant, on sait que les réseaux privés militaire, des étrangers et de l'élite offrent un accès international⁹⁵³ (par le biais de l'AS20485 de TTK en Russie et l'AS134544 de Cenbong Int'l Holdings Ltd à Hong-Kong), tandis que le réseau privé civil n'a pas le droit d'offrir un tel accès⁹⁵⁴. On a donc supposé que les réseaux privés militaire, des étrangers et de l'élite appartiennent à des sous-réseaux différents du ou des sous-réseaux dont relève le réseau civil. Par ailleurs, pour des raisons de sécurité, on imagine mal que la porte d'accès au réseau des étrangers et de l'élite soit la même que celle pour accéder au réseau militaire, raison pour laquelle on considère qu'ils ne relèvent probablement pas du même sous-réseau. Enfin, compte tenu du nombre du nombre de machines connectées par le Kwangmyong – probablement le plus grand réseau privé de l'internet nord-coréen –, on a fait l'hypothèse que le nombre de routeurs et donc d'adresses publiques nécessaire pour transmettre correctement le trafic à travers les grandes villes et leurs périphéries exige au moins 512 adresses IP publiques, soit deux sous-réseaux de 256 adresses IP publiques. Cette hypothèse est très discutable, d'autant que nous n'avons pu évaluer la qualité du trafic nord-coréen. Pour ces raisons, on a inclus les adresses IP publiques des réseaux privés de l'élite et des étrangers (ambassades, ONG, touristes) dans le sous-réseau 1, celles du réseau privé militaire dans le sous-réseau 4, et on a réservé les sous-réseaux 2 et 3 aux adresses IP publiques du réseau civil.

Par « réseau militaire nord-coréen », on désigne l'ensemble des machines spécialement dédiées à des opérations militaires nord-coréennes. Ce réseau admet probablement les machines utilisées pour la cyberdéfense et la cyberguerre nord-coréennes. Dès 1998, la Corée du Nord a établi l'Unité 121 comme l'administration chargée de la cyberguerre⁹⁵⁵. Au milieu des années 2000, la Corée du Nord fait de la cyberguerre un axe de sa politique militaire : « en 2005, un livre de l'Armée populaire coréenne citait Kim disant : »si Internet est comme une arme à feu, les cyberattaques sont comme des bombes nucléaires « »⁹⁵⁶. L'Unité 121, qui relevait jusqu'à présent de l'état-major de l'Armée populaire de Corée, est intégrée en 2009 au sein d'un nouveau service de renseignement issu de la fusion de quatre grands services de renseignement en un seul : le Bureau général de reconnaissance (정찰총국, *Reconnaissance General Bureau*, RGB) spécialisé dans le renseignement extérieur⁹⁵⁷. Cette date marque le déploiement de l'Unité 121. En même temps qu'elle intègre le RGB, son rang administratif est rehaussé – d'« Unité », elle devient un « Bureau ». Ses effectifs augmentent à 3 000 personnes, contre les 500 à 1000 agents dont il disposait jusqu'à présent⁹⁵⁸.

En 2013, le Bureau 121 s'enrichit d'une nouvelle division, l'Unité 180 dotée de 500 employés et chargée des opérations de transferts illicites d'argent⁹⁵⁹. Par exemple, en 2016, l'Unité 180 est la première suspecte d'un braquage de la Banque centrale du Bangladesh par

953 TALMADGE Eric, « North Korea's digital divide: Online elites, isolated masses » [en ligne], *Chicago Tribune*, nov. 2017

954 DUFFLEY Robert, « Information Technology and Control in the DPRK » [en ligne], *Cornell International Affairs Review*, vol. 5, 2011, p. 47-53

955 PAPAIN Tom, « North Korea and Cyberwarfare: How North Korea's Cyber Attacks Violate the Laws of War », *Journal of Korean Law*, vol. 11, 2011, p. 29-54

956 CAESAR Ed, « The Incredible Rise of North Korea's Hacking Army » [en ligne], *The New Yorker*, 2021

957 RASKA Michael, « North Korea's Evolving Cyber Strategies: Continuity and Change », *SIRIUS – Zeitschrift für Strategische Analysen*, vol. 4, no. 2, 2020, p. 1-13

958 *Ibid.*

959 *Ibid.*

cyberattaque pour un montant de 81 millions de dollars⁹⁶⁰. Vers 2014-2015, les missions de l'Unité 180 se spécialisent vers les braquages de plateformes d'échange de cryptomonnaies : en janvier 2018, l'Unité 180 semble être l'auteur d'une cyberattaque dirigée contre la plateforme Tokyo Coincheck pour vol de cryptomonnaies équivalant à 530 millions de dollars⁹⁶¹ ; en avril 2022, elle est suspectée par les services de renseignement américain d'être l'auteur de la cyberattaque contre la plateforme Axie Infinity pour un vol de cryptomonnaies équivalant à 615 millions de dollars⁹⁶² ; elle est aussi suspectée de la cyberattaque dirigée le même jour contre le réseau Ronin pour un vol de cryptomonnaies équivalant à 540 millions de dollars⁹⁶³. Cette activité de l'Unité 180 est un important gisement financier pour la Corée du Nord afin de contourner les sanctions économiques internationales. Outre l'Unité 180, deux autres divisions composent le Bureau 121. D'une part, le laboratoire de recherche en technologie informatique du RGB (Lab 110) est « censé fournir du génie logiciel, de la surveillance technique, de l'infiltration de réseaux informatiques, de la collecte de renseignements par le piratage et de l'installation de virus sur des réseaux ciblés. (...) Le Lab110 analyse la configuration technologique et les modèles de comportement des cibles, puis développe des logiciels et des malwares sur mesure, qui sont ensuite utilisés par les cyberattaques du Bureau 121 »⁹⁶⁴. D'autre part, l'Unité 91 est chargée du « cyber-espionnage des technologies nécessaires au développement des programmes nucléaires et de missiles balistiques de la Corée du Nord »⁹⁶⁵. Coiffant tout un arsenal administratif (Unité 180, Lab 110, Unité 91) dédié aux opérations militaires extérieures sur le réseau internet, le Bureau 121 et ses divisions forment proprement une cyber-armée. En 2020, le renseignement américain évaluait à 6 000 le nombre d'agents du Bureau 121⁹⁶⁶. Les membres du Bureau 121 sont choisis par l'État parmi les élèves les plus brillants d'au moins quatre universités de Pyongyang : l'Université Kim Il-sung, l'Université de technologie Kim-Chaek, l'Université de Moranbong et l'Université des sciences et des technologies de Pyongyang (PUST)⁹⁶⁷.

Cette cyber-armée du RGB est complétée par deux autres : celle de l'état-major général de l'Armée populaire de Corée ; et la milice Lazarus. Depuis l'intégration du Bureau 121 dans le RGB en 2009, l'état-major général de l'Armée populaire de Corée n'exerce plus d'autorité directe sur ce Bureau. Il gère néanmoins un autre Bureau, le Bureau d'automatisation du

960« The Lazarus heist: How North Korea almost pulled off a billion-dollar hack » [en ligne], *BBC*, juin 2021

961« South Korean intelligence says N. Korean hackers possibly behind Coincheck heist » [en ligne], *Reuters*, 5 fév. 2018

962« Le FBI accuse la Corée du Nord d'avoir piraté le jeu de cryptomonnaies « Axie Infinity », *Courrier International*, 15 avr. 2022

963UTERSINGER Martin, Le FBI accuse la Corée du Nord du vol de 540 millions de dollars dans le réseau de cryptomonnaie Ronin, *Le Monde*, 15 avr. 2022

964RASKA M., « North Korea's Evolving Cyber Strategies: Continuity and Change », *SIRIUS – Zeitschrift für Strategische Analysen*, préc.

965Ibid.

966Département de l'Armée des États-Unis, *North Korean Tactics* [rapport en ligne], Army Techniques Publications No. 7-100.2, juil. 2020

967LEE Daehee, « Les "hackers d'élite" de la Corée du Nord se livrent à un cyberharcèlement de devises étrangères » (北 '엘리트 해커' 사이버 외화벌이), *Nocutnews.co.kr* [journal sud-coréen], août 2011 ; AHN JH et YORK Rob, « Are PUST students potentiel North korean hackers ? » [en ligne], *NKNews* [journal américain sur l'actualité nord-coréenne], déc. 2015

commandement (Command Automation Bureau)⁹⁶⁸. Ce Bureau ne mène pas les opérations sur le terrain contrairement au Bureau 121, mais développe des logiciels malveillants (à travers son Unité 31), des logiciels à usage militaire (à travers son Unité 32) et des logiciels destinés au commandement et au contrôle militaires (à travers son Unité 56)⁹⁶⁹. Les deux cyber-armées du RGB (Bureau 121 et ses divisions) et de l'état-major général de l'Armée populaire de Corée (Bureau d'automatisation du commandement et ses divisions) sont enfin aidées par une cyber-milice couramment surnommée « Lazarus » par les autorités de cybersécurité. Lazarus désigne une nébuleuse de groupes de hackers qui œuvrent pour l'intérêt de l'État nord-coréen, dont APT37 (spécialisée dans le vol d'informations des réseaux industriels et militaires étrangers, notamment en Corée du Sud et au Japon), APT38 (cyber-attaques contre les) Kimsuky (cyber-espionnage des organisations gouvernementales et militaires étrangères), Sun Team (cyberattaques contre les appareils des transfuges nord-coréens ayant fait défection et des journalistes sud-coréens) et AndAriel (cyber-espionnage des organisations militaires sud-coréennes, des instituts étrangers de recherche sur l'énergie, des sociétés de sécurité, des plateformes d'échange de crypto-monnaies et de jeux d'argent en ligne, des banques...)⁹⁷⁰.

Lazarus, le Bureau 121 et l'Unité 180 se coordonnent régulièrement pour mener des opérations sur de nombreux fronts : pour protéger l'image de l'État (cyberattaque ayant détruit 70% des ordinateurs portables de Sony Picture en 2014 pour avoir distribué le film *The Interview* parodiant Kim Jong-un⁹⁷¹, cyberattaque la même année contre le réseau de télévision publique britannique Channel Four pour avoir annoncé une série mettant en scène un chercheur britannique en physique nucléaire enlevé à Pyongyang⁹⁷²...) ; pour les vols bancaires ou de cryptomonnaies déjà étudiés ; pour espionner des réseaux d'entreprise étrangères (cyberattaque en septembre 2022 contre la bibliothèque logicielle open source Log4j⁹⁷³), des gouvernements (Operation Troy dirigée entre 2009 et 2012 contre le gouvernement sud-coréen⁹⁷⁴) ou des armées étrangères (Operation Plan 5015 dirigée en 2016 contre l'armée sud-coréenne pour voler des données militaires⁹⁷⁵) ; ou encore pour des fins ambiguës (on ignore par exemple les raisons ayant conduit Lazarus à créer et à diffuser le rançongiciel Wannacry en 2022). Les agents du Bureau 121 n'opèrent pas seulement sur le territoire nord-coréen, mais semblent avoir des locaux en Biélorussie, en Chine, en Inde, en Malaisie et en Russie voire dans davantage de pays⁹⁷⁶. **Le réseau privé militaire de l'internet nord-coréen est aujourd'hui indispensable au régime pour contourner les sanctions économiques internationales, pour atteindre les objectifs du juche** (idéologie d'État reposant sur les trois objectifs de l'indépendance politique (자주), de l'autosuffisance

⁹⁶⁸RASKA M., « North Korea's Evolving Cyber Strategies: Continuity and Change », préc.

⁹⁶⁹*Ibid.*

⁹⁷⁰ *Ibid.*

⁹⁷¹HORNADAY Ann, « Sony, 'The Interview' and the unspoken truth: All movies are political », *Washingtonpost.com*, déc. 2014

⁹⁷²SANGER David E., KIRKPATRICK David D. et PERLROTH Nicole, « The World Once Laughed at North Korean Cyberpower. No More. » [en ligne], *The New York Times*, oct. 2017

⁹⁷³PAGE Carly, « North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies » [en ligne], *TechCrunch*, août 2022

⁹⁷⁴SHERSTOBITOFF Ryan et LIBA Itai, « Dissecting Operation Troy: Cyberespionage in South Korea », White Paper pour l'entreprise McAfee [PDF en ligne]

⁹⁷⁵JI-HYE Jun, « JCS refuses to share new wartime plan with Assembly » [en ligne], *The Korea Times*, oct. 2015

⁹⁷⁶Healthcare Sector Cybersecurity Coordination Center (HC3), « North Korean Cyber Activity » [en ligne]. *U.S. Department of Health & Human Services*, mars 2021, p. 14

économique (자립) et de l'autonomie militaire (자위)) **et pour démontrer géopolitiquement la puissance technique du pays malgré sa pauvreté**⁹⁷⁷.

Pour ses activités, le réseau privé militaire doit pouvoir accéder au réseau international, d'où la connexion de l'AS Ryugyong-dong à l'opérateur russe TTK et à l'opérateur sino-hongkongais Cenbong. De même, l'élite nord-coréenne (hauts-fonctionnaires, cadres du Parti des Travailleurs, certains journalistes...) bénéficie aussi d'un accès au réseau international mais de façon restreinte : sont bloqués et/ou filtrés les accès aux sites internet pornographiques, d'informations relatives aux drogues, de jeux d'argent, aux réseaux sociaux Facebook, Twitter, Instagram et YouTube ainsi qu'aux sites internet sud-coréens, à toutes plateformes de vidéos à la demande (Netflix, Amazon Prime, CBS...), et à la quasi-totalité des médias étrangers d'information⁹⁷⁸. Les services étrangers illicites dont l'accès est empêché pour l'élite sont traqués – à des fins de blocage ou de filtrage – par les Groupes 109, 114 et 118, des administrations chargées de faire appliquer notamment les articles 183, 184 et 185 du Code pénal proscrivant la diffusion des cultures et actes décadents ou hostiles⁹⁷⁹. L'élite semble en revanche avoir accès à Google, Alibaba, Amazon, Youku, Baidu, iTunes, et la plupart des services et jeux en ligne⁹⁸⁰.

Inversement, l'accès au réseau international est bloqué ou filtré pour les utilisateurs du réseau privé civil (Kwangmyong). Or, si les routeurs constitutifs des réseaux militaires et de l'élite offrent un accès international alors que les routeurs constitutifs du réseau civil n'en offrent pas, cela suppose que **les routeurs du réseau civil bloquent ou filtrent très probablement l'accès aux routeurs des autres réseaux privés**, i.e. empêchent l'acheminement de toute requête

⁹⁷⁷ L'un des principaux économistes du régime politique nord-coréen, Ri Ki Song, résume en 2018 les enjeux de la démonstration de force militaire nord-coréenne. Dans le cadre du documentaire d'Arte « Les Hommes de Kim » ayant reçu le prix Albert Londres 2018, la journaliste Marjolaine Grappe questionne le professeur : « *la Corée du Nord n'aurait-elle pas intérêt à abandonner le développement des armes nucléaires et à ce que les sanctions des Nations-Unies soient levées ?* ». Le professeur répond : « *c'est un enjeu qui nécessite une compréhension profonde de l'histoire. Les États-Unis nous ont déclaré la guerre le 28 juin 1950. Trois jours après, en passant une loi sur le contrôle des exportations, ils ont bloqué toutes les exportations en provenance de Corée du Nord. La même année, en décembre, ils ont passé une loi pour nous désigner comme pays ennemi et nous interdire tout commerce. Ce qui veut dire que même à l'époque où nous n'avions pas d'armes nucléaires, les États-Unis n'avaient de cesse que de nous suffoquer économiquement. Il n'y qu'en étant supérieurs aux américains avec nos armes nucléaires que nous pouvons assurer un développement économique. Maintenant qu'ils ne peuvent plus nous menacer, même avec leurs armes, nous sommes enfin en mesure de procéder au développement économique sans inquiétude. Qu'est-ce que vous en pensez ?* ».

⁹⁷⁸ TALMADGE Eric, « North Korea announces blocks on Facebook, Twitter and YouTube » [en ligne], *The Guardian*, 1 avril 2016

⁹⁷⁹ Le groupe 118 est spécialisé dans la lutte contre les services d'informations relatives aux drogues (et contre la possession et le trafic de drogues en général) ; le groupe 109 est spécialisé dans la lutte contre les informations étrangères illicites (diffusion ou consommation de films ou de médias étrangers d'information), et peut mener à cette fin des perquisitions « *y compris la nuit pendant que les occupants dorment* » pour vérifier si les clés USB ou autres matériaux électroniques ne stockent pas des informations décadentes ; le groupe 114 complète le groupe 109 dans la lutte contre les « *"médias impurs" principalement étrangers* » et la surveillance des transfuges nord-coréens ayant fui le territoire. V. WILLIAMS Martyn, « Digital Trenches. North Korea's Information Counter-Offensive », *Committee for Human Rights in North Korea (HKRN)*, préc., 2019, p. 16

⁹⁸⁰ TIMBERG Craig et NAKASHIMA Ellen, « Not so isolated » [en ligne], *Washington Post*, 25 juil. 2017

provenant de ou destinée à une adresse IP publique non dédiée à Kwangmyong. De cette façon, aucune adresse IP publique membre de Kwangmyong ne peut communiquer avec une adresse IP publique non-membre de Kwangmyong : une adresse IP privée membre de Kwangmyong ne peut pas accéder à une adresse IP privée membre du réseau militaire ou de l'élite par le biais du réseau public ; elle ne peut pas non plus accéder à une adresse IP publique étrangère ; et pareillement, aucune machine étrangère ne peut accéder à Kwangmyong dès lors que son adresse IP publique appartient à un autre réseau que Kwangmyong. Dans cette logique d'un réseau civil fermé sur lui-même, il est par ailleurs très probable que les serveurs fournissant les services en ligne de Kwangmyong (moteur de recherche, forums, sites de vente en ligne...) soient eux-mêmes rattachés à des adresses IP publiques dédiées à Kwangmyong – on ne voit pas, autrement, comment les terminaux membres de Kwangmyong pourraient y accéder dès lors que les routeurs du Kwangmyong semblent refuser d'acheminer les requêtes de ces terminaux vers d'autres adresses IP publiques que celles dédiées au réseau civil.

On tire plusieurs leçons sur la structure des réseaux IP et d'acheminement nord-coréens. Premièrement, les réseaux privés identifiés de l'internet nord-coréen sont isolés les uns des autres. Ce cloisonnement des réseaux privés dû au fait que les routeurs d'un réseau privé semblent empêcher l'accès aux routeurs des autres réseaux privés⁹⁸¹. Il est aussi facilité par le très faible nombre d'adresses IP publiques, ce qui simplifie sa mise en œuvre. L'accès au réseau international est gradué selon le réseau privé concerné grâce à ce cloisonnement. Deuxièmement, le réseau civil est un intranet *i.e.* un même réseau privé connectant un grand nombre d'utilisateurs, et non une interconnexion de plusieurs réseaux privés comme c'est le cas dans tous les autres pays fournissant un accès internet à notre connaissance. Cette concentration du réseau civil dans un seul réseau privé est due au cloisonnement des réseaux privés, soit au filtrage et au blocage de la communication entre les adresses IP publiques dédiées au réseau civil et les adresses IP publiques dédiées aux autres réseaux privés. Troisièmement, le réseau civil est imperméable à tout accès provenant de ou destiné à une machine étrangère. Cette imperméabilité est due au fait que les routeurs de Kwangmyong n'acheminent probablement que les requêtes dont la provenance ou la destination renvoient à une adresse IP publique membre de Kwangmyong. Quatrièmement, un seul opérateur (Star JV) peut définir : quel réseau privé peut accéder à quel autre réseau privé membre du réseau national ; quel réseau privé, sous-réseau ou adresse IP privée peut accéder à un AS étranger ; et quelle adresse IP privée peut être interdite d'accès. Cette centralisation de la gestion est due au fait que le réseau national de l'acheminement relève du seul opérateur Star JV appartenant à l'État. Cinquièmement, l'accès étranger au réseau nord-coréen est particulièrement difficile. Ce niveau de difficulté est dû au fait que le réseau IP nord-coréen est composé d'un seul AS, de façon à limiter le nombre de portes d'accès de l'ensemble du réseau à seulement quatre sous-réseaux au trafic étroitement contrôlé par Star JV.

À l'issue de notre examen de la centralisation de divers réseaux nationaux de transport (France, Royaume-Uni, États-Unis, Russie Chine, Corée du Nord, Iran), on en conclut que la technique de la centralisation présente plusieurs avantages et inconvénients. On lui reconnaît deux avantages de taille. D'abord, en établissant un goulot d'étranglement qui rapporte un grand nombre de nœuds émetteurs à un petit nombre de nœuds destinataires, la centralisation permet d'appliquer

⁹⁸¹ On émet toutefois un doute sur le cloisonnement total du réseau militaire et du réseau civil ; peut-être les routeurs admettent-ils certaines adresses IP publiques issues du réseau militaire pour permettre une surveillance de Kwangmyong par l'Armée

à tous les émetteurs des mesures mises en œuvre par quelques destinataires seulement. Autrement dit, **la centralisation a pour premier avantage** de rendre possible l'application de mesures techniques à la communauté d'émetteurs qui dépend du destinataire central, *i.e.* **de généraliser l'exécution des techniques de régulation** (ralentissement, blocage, filtrage, coupure...) **à une échelle collective**. Par exemple, en Corée du Nord, la centralisation des voies nationales et internationales d'accès IP par Star JV permet à ce dernier de définir les connexions entre réseaux privés et avec des AS étrangers. En Chine, la centralisation des voies nationales et internationales d'acheminement par cinq grands opérateurs (China Telecom, China Unicom, China Mobile, 21 Viannet, ministère de l'Éducation avec CERNET) permet de restreindre tout accès aux réseaux étrangers depuis le réseau national. En Russie, la centralisation des voies nationales et internationales d'accès sous-marin permet d'assurer la totalité du trafic sous-marin national en cas d'isolement. En limitant la diversité des voies d'accès, **la centralisation a pour deuxième avantage de limiter les possibilités et donc les risques de contournement** : plus les voies d'accès sont diversifiées, plus les prescripteurs ont d'alternatives pour contourner la restriction ; moins elles sont diversifiées, moins les prescripteurs ont d'alternatives à leur disposition pour contourner la restriction. Par conséquent, **une combinaison de la centralisation avec d'autres techniques de restriction a pour effet de compenser** – dans la mesure de la centralisation – **l'un des inconvénients du blocage, du filtrage et du ralentissement**, à savoir la facilité de leur contournement, et **donc d'augmenter l'efficacité de ces techniques**.

Le premier inconvénient de la centralisation découle de ses avantages : la centralisation n'a pas en elle-même pour effet de réduire l'échelle de diffusion d'une R-DATA, *i.e.* de réduire le nombre de machines différentes qui produisent ou stockent (accèdent à) cette R-DATA. Si le réseau centralisé sans le moindre blocage, filtrage, coupure ou ralentissement de l'accès à une R-DATA, les prescripteurs pourront continuer d'accéder à cette R-DATA pour amplifier son échelle de diffusion. La technique de la centralisation n'a donc pas d'efficacité en elle-même sur l'échelle de diffusion d'une R-DATA si elle n'est pas accompagnée d'une autre technique de restriction. Le deuxième inconvénient de la centralisation est bien plus problématique. En faisant dépendre un grand nombre de nœuds émetteurs d'un petit nombre de nœuds destinataires, la centralisation fait de ces destinataires des nœuds critiques du réseau. Un accident affectant un nœud central (une cyberattaque, une erreur du gestionnaire du nœud ou d'un de ses agents) touchera tous les émetteurs qui en dépendent. Autrement dit, **la centralisation a pour deuxième inconvénient d'aggraver la vulnérabilité d'un réseau**. Plus un réseau est centralisé, plus il est uniformisé par un faible nombre de nœuds centraux devenant des nœuds critiques, plus la moindre défaillance d'un nœud critique provoque celle du réseau dans la mesure du réseau couverte par ce nœud. Par exemple, en février 2022, un hacker américain est parvenu à lui seul à paralyser la totalité de l'internet nord-coréen en exploitant des vulnérabilités communes à tous les routeurs et serveurs nord-coréens⁹⁸². *A contrario*, l'effondrement d'un internet national est peu concevable dans un réseau très décentralisé, car un tel effondrement nécessiterait de faire s'écrouler un grand nombre de nœuds très divers (y compris dans leurs vulnérabilités respectives).

⁹⁸² GREENBERG Andy, « North Korea Hacked Him. So He Took Down Its Internet » [en ligne], *Wired*, 2 fév. 2022. Le hacker a principalement agi dans le cadre d'une attaque par déni de service, et a refusé de dévoiler la plupart des vulnérabilités exploitées. Il a néanmoins décrit l'une d'entre elles, déjà connue, du logiciel NginX avec lequel sont programmés les serveurs en Corée du Nord, qui gère mal certains en-tête HTTP.

Paragraphe 2 – La centralisation du stockage de données : l'exemple des noms de domaine

À la fois centralisé par son gestionnaire qu'est l'Icann, et décentralisé par son fonctionnement, le système des noms de domaines se trouve dans un entre-deux (A). Désireuse de quitter cette gestion centralisée par l'Icann et de reprendre la main sur son réseau national, la Russie a isolé son propre système national de noms de domaine (B).

A) Centralisation et décentralisation du réseau DNS

Après avoir examiné la centralisation du réseau internet dès les infrastructures réseau – câbles sous-marins et routeurs –, on s'attarde ici sur la centralisation du réseau internet dès le stockage de données. On a vu que **les machines de transmission** (transport et acheminement) **établissent un réseau**, tandis que **les machines de stockage en ligne** (serveurs, terminaux et périphériques accessoires) **utilisent le réseau établi pour y stocker des données**. On distingue deux types de machines de stockage en ligne : les machines de stockage bref, qui stockent les données reçues pour le temps minimal à leur traitement avant la transmission de ces dernières (résolveurs DNS, serveurs DHCP, serveurs VPN⁹⁸³...) ; et les machines de stockage long, qui stockent les données reçues pour un temps supérieur à leur traitement (terminaux, serveurs cloud ou de collecte, objets connectés...). Que leur stockage soit bref ou long, ces machines ne peuvent stocker des données en ligne qu'en étant connectées à un réseau établi par des machines de transmission. Comme les machines de transmission, les machines de stockage en ligne peuvent faire l'objet d'une centralisation. On étudie la centralisation dès les serveurs de noms de domaine.

On sait déjà que la gestion des adresses IP publiques est mondialement centralisée par l'Icann. Cette centralisation se traduit sur le plan opérationnel par l'obligation, pour tous les FAI dans le monde, de se voir allouer des plages d'adresses IP publique de la part de l'Icann, pour que leur propre réseau soit doté d'une adresse IP qui le situe sur le réseau public et pour attribuer des adresses IP publiques aux réseaux locaux de leurs abonnés. Elle se traduit ensuite sur le plan de la gestion par la compétence exclusive de l'Icann pour garantir la cohérence de toutes les adresses IP stockées sur ses serveurs racines, et donc pour assurer le bon fonctionnement du réseau (des adresses IP manquantes ou inexactes peuvent empêcher l'accès par des machines à d'autres machines connectées au réseau). Elle se traduit enfin sur le plan du trafic par le fait que toute requête transportée sur le réseau public doit emprunter les serveurs racine de l'Icann.

Cette centralisation s'explique par l'histoire d'internet. À sa naissance en 1977, internet interconnectait trois réseaux selon le protocole TCP/IP : ARPANET (qui exploitait les lignes téléphoniques d'AT&T), le réseau satellitaire SATNET et le réseau hertzien. La gestion des adresses IP revenait alors de fait au gestionnaire des infrastructures d'ARPANET, à savoir l'ARPA (devenue DARPA, *Defense Advanced Research Projects Agency*, une agence gouvernementale qui se consacre à la recherche technologique à des fins militaires). En 1987, les premiers réseaux étrangers se connectent au réseau dorsal d'ARPANET en se servant eux-mêmes du protocole TCP/IP. La politique de gestion des adresses IP devient alors une question internationale qui ne peut plus relever du seul Département américain de la défense⁹⁸⁴. En 1988, à la demande d'un des

⁹⁸³ Les serveurs de noms de domaine (DNS) associent une appellation syntaxique à un service stocké en ligne ou à tout autre membre du réseau. Les serveurs *Dynamic Host Configuration Protocol* (DHCP) complètent les serveurs DNS en associant une adresse IP et un masque sous-réseau à toute machine qui accède au réseau internet public. Quant aux serveurs VPN, on a déjà décrit leur rôle et leur fonctionnement.

⁹⁸⁴ BAMDE Aurélien, *L'architecture normative du réseau internet*, 2014, préc., p.370

premiers participants aux développements d'internet – Jon Postel –, la DARPA transfère la gestion des adresses IP et des noms de domaine à une nouvelle autorité dirigée par Jon Postel : l'*Internet Assigned Numbers Authority* (IANA)⁹⁸⁵. Organisme fédéral sous partenariat avec le Département américain du commerce, l'IANA transfère en 1999 la gestion des adresses IP et noms de domaine à l'Icann, une société privée à but non lucratif. La pression des États de tout bord contre les États-Unis conduit le Département américain du commerce à libérer l'Icann de sa tutelle en 2016⁹⁸⁶, faisant de l'Icann une société juridiquement indépendante du gouvernement américain et de tout autre gouvernement.

On voit donc deux raisons contraires expliquant la centralisation mondiale de la gestion des adresses IP publiques : les réseaux étrangers ont commencé à utiliser le protocole réseau (TCP/IP) d'une administration américaine (DARPA) dont les adresses IP étaient alors exclusivement attribuées par cette administration ; et une fois internet déployé mondialement, les États se sont entendus pour qu'aucun État ne centralise à lui seul la gestion des adresses IP. Par conséquent, la centralisation mondiale des adresses IP publiques a d'abord été une centralisation étatique des États-Unis (de 1977 à 2016), avant de devenir une centralisation inter-étatique depuis 2016. Malgré le rôle des États dans cette centralisation, la gouvernance privée des adresses IP peut puissamment dépasser le pouvoir des États sur leur internet national : l'Icann peut techniquement couper tout accès internet dans un ou plusieurs territoires, par exemple en refusant d'allouer des adresses IP publiques aux opérateurs de ce pays ou encore en supprimant de ses serveurs racine toutes les adresses IP publiques allouées à ce pays⁹⁸⁷. Dès lors, la centralisation mondiale de la gestion des adresses IP est très hybride : bien qu'elle soit d'initiative inter-étatique, les États ont, même collectivement, très peu d'emprise sur cette gestion pratiquée par une société privée à but non lucratif⁹⁸⁸.

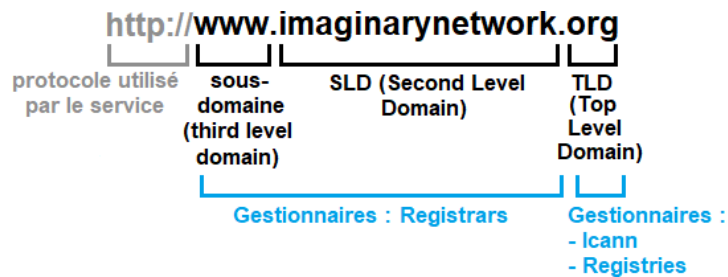
Cette centralisation hybride de la gestion des noms de domaine engendre une centralisation elle aussi hybride du réseau des serveurs de noms de domaine (« réseau DNS »). Le réseau DNS est constitué de deux types de serveurs : les serveurs DNS faisant autorité (*authoritative name servers*) ; et les résolveurs DNS (ou serveurs de résolution de noms de domaine, *caching name servers*). Les serveurs DNS faisant autorité stockent durablement les noms de domaine dans le but de les rendre constamment disponibles en ligne. Or, on a vu qu'un nom de domaine est ainsi morcelé :

985Ibid. p. 371

986« Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends », *Icann.org*, 1^{er} oct. 2016

987On pense entre autres à un précédent, qui concernait non les adresses IP mais les noms de domaine attribués par l'Icann : entre 2002 et 2005, l'Icann avait suspendu le geoTLD <.iq> (geoTLD irakien) alors que les États-Unis accusaient le dépositaire du <.iq> de complicité avec des organisations terroristes et que l'Icann jugeait le pays trop instable après la guerre pour pouvoir gérer son propre geoTLD (BEST Jo, « Iraq gets its own domain name back », sur *ZDNET* [en ligne], 8 août 2005 [consulté le 5 septembre 2022] ; et Sénat français, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Rapport d'information n° 696, 8 juil. 2014, p. 97)

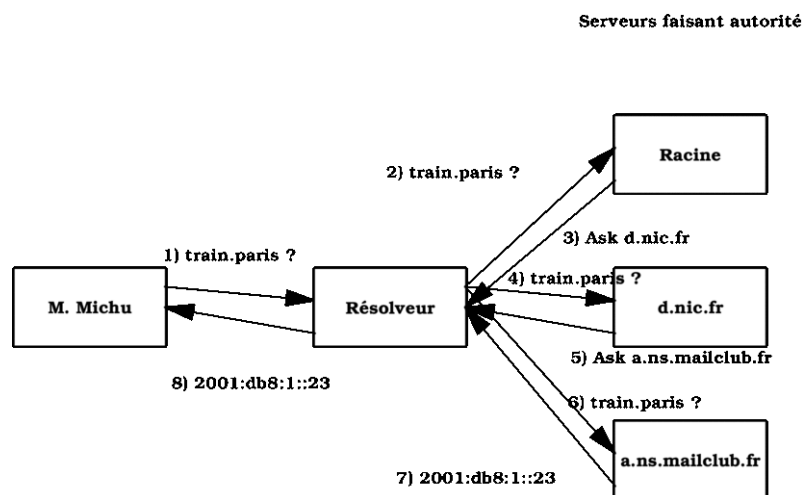
988Les États y ont leur place au sein du *Governmental Advisory Committee* – section interétatique de l'Icann –, mais leurs avis sont consultatifs auprès du conseil d'administration de l'Icann



Un nom de domaine inclut un sous-domaine (`www.`, `blog.`, `forum.`, `google.` etc.), un SLD (`imaginarynetwork` dans notre exemple) et un TLD (`.org` ici). Les registrars stockent sur leurs serveurs (« serveurs d'enregistrement ») les SLD et les sous-domaines demandés par le candidat à l'obtention d'un nom de domaine. **Toute requête qui souhaite accéder aux morceaux <www.imaginarynetwork> devra donc emprunter les serveurs du registrar qui stocke lesdits morceaux.** Quant aux TLD, l'Icann en est le gestionnaire de principe : tous les TLD sans exception sont stockés sur les serveurs de l'Icann dits « serveurs racines ». **Toute requête qui souhaite accéder à un TLD doit donc emprunter les serveurs racines de l'Icann.** Les TLD sont de quatre type : les TLD génériques (gTLD comme `<.com>`, `<.org>`, `<.net>`, `<.info>`, `<.app>`, `<.blog>`, `<.airbus>`, `<apple>`, `<.bnpparibas>`...) ; les TLD génériques restreints (restricted TLD `<.biz>`, `<.name>`, `<.pro>`) ; les TLD génériques locaux (geoTLD comme `<.paris>`, `<.berlin>`, `<.wales>`...) ; les TLD nationaux (country code TLD ou ccTLD comme `<.fr>`, `<.uk>`, `<.cn>`, `<.ca>`, `<.io>`...) ; et les TLD sponsorisés (sponsored TLD `<.gov>`, `<.edu>`, `<.mil>` pour militaire, `<.museum>`, `<.travel>`, `<.coop>`...). Enfin, on a vu que l'Icann délègue la gestion de la quasi-totalité des TLD à des registries : l'Afnic gère les `<.fr>` et `<.paris>`, VeriSign gère les `<.com>` et `<.net>`, le Département de la Sécurité Intérieure des États-Unis gère le `<.gov>` à travers la Cybersecurity and Infrastructure Security Agency etc. Chacun de ces registries copie une partie des serveurs racine de l'Icann sur ses propres serveurs afin d'y répliquer les informations relatives au(x) TLD dont ils ont la gestion. **Toute requête qui souhaite accéder à un TLD délégué doit donc emprunter les serveurs TLD du registry auquel est délégué la gestion de ce TLD.**

Tout nom de domaine est ainsi fractionné en plusieurs tronçons, et chaque tronçon est stocké sur un serveur différent (serveur racine, serveur TLD du registry et serveur d'enregistrement du registrar). Ces serveurs DNS qui stockent durablement des tronçons de noms de domaine font autorité sur le deuxième type de serveur membre du réseau DNS : les résolveurs DNS. Pour en comprendre le fonctionnement, on s'aidera du schéma proposé par l'informaticien et universitaire Stéphane Bortzmeyer⁹⁸⁹ :

989BORTZMEYER Stéphane, « Serveur DNS faisant autorité : définition », sur *Bortzmeyer.org*, 11 mai 2020 [consulté le 30 sept. 2022]

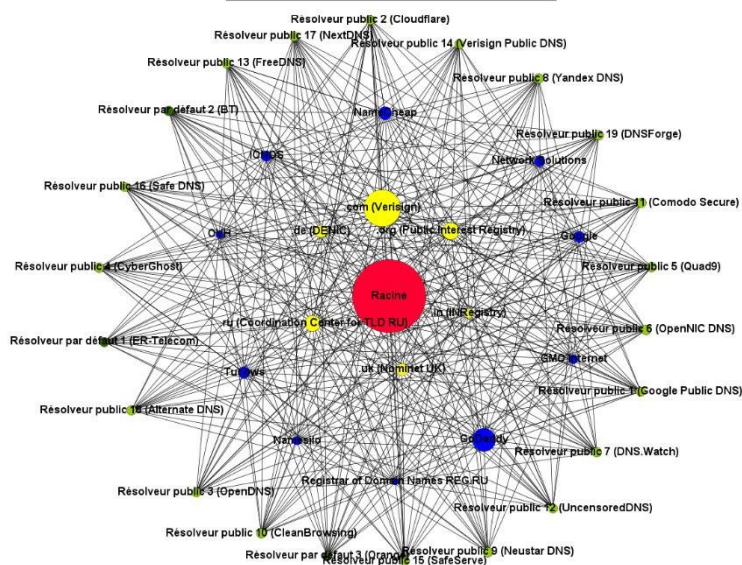


Dans cet exemple, l'utilisateur M. Michu souhaite accéder au site `<train.paris>` dont le geoTLD est géré par l'Afnic. Il émet une requête posant la question « *comment accéder au site internet possédant ce nom de domaine ?* » destinée au résolveur DNS. Le résolveur interroge tour à tour chacun des serveurs faisant autorité sur la question, à savoir le serveur racine dans tous les cas, le serveur TLD de l'Afnic (d.nic.fr) gestionnaire du `<.paris>` et le serveur d'enregistrement sur lequel est hébergé le nom de domaine de `<train.paris>` (a.ns.mailclub.fr). Chaque serveur faisant autorité communique sa réponse au résolveur, aboutissant à la communication par le serveur d'enregistrement de l'adresse IP du serveur sur lequel est hébergé le nom de domaine de `<train.paris>`. Le résolveur peut alors apporter une réponse à la question posée et renverra au terminal de M. Michu l'adresse IP lui donnant accès au site internet requis.

Les résolveurs DNS sont donc des serveurs intermédiaires reliant le terminal et les serveurs DNS faisant autorité. À la différence des serveurs DNS faisant autorité, qui stockent durablement les noms de domaine, les résolveurs DNS sont des machines de stockage bref qui stockent les noms de domaine généralement 30 à 300 secondes, le temps de leur « durée de vie » (*time to live* ou TTL, indiqué dans l'en-tête du nom de domaine dès sa création⁹⁹⁰). Surtout, à la différence des registrars, les résolveurs DNS ne dépendent pas d'une validation par l'Icann (*registrar agreements*) pour fournir leur service. Tout FAI fournit à ses utilisateurs un résolveur DNS par défaut à ses abonnés, mais les abonnés peuvent choisir d'emprunter un résolveur DNS dit « public » proposé par un fournisseur tiers (Cloudflare, Google Public DNS, NextDNS...). Les résolveurs DNS publics ont pour intérêt de sécuriser et d'accélérer l'accès à un nom de domaine, et le cas échéant de contourner la politique d'un FAI sur les noms de domaine (par exemple, blocage ou filtrage de noms de domaine par l'opérateur, surveillance du trafic...).

⁹⁹⁰ Plus le TTL d'un nom de domaine est long, plus sont élevées les chances d'accéder au nom de domaine stocké (« mis en cache ») par le résolveur, plus seront accélérées les requêtes DNS d'accès à ce nom de domaine

Modélisation du réseau DNS (échelle minimale)



On a modélisé ci-contre ce réseau DNS à une échelle minimale. On situe en bordure du réseau les résolveurs DNS (en vert clair pour les résolveurs publics et en vert foncé pour les résolveurs que les FAI fournissent par défaut). Sur le schéma, ces résolveurs forment un cercle vert à l'intérieur duquel trois autres cercles prennent place – bleu, jaune et rouge. Ces trois cercles sont formés par les serveurs DNS faisant autorité : les nœuds bleus représentent les serveurs d'enregistrement des registrars ; les nœuds jaune représentent les serveurs TLD des registries ; le nœud rouge représente les serveurs racines de l'Icann. Les morceaux d'un même nom de

domaine sont répartis entre deux (racine et registrar) voire trois (serveurs TLD) de ces trois cercles, chacun de ces cercles étant géré par un type différent de gestionnaire (registrars, Icann, registry). Les liens représentent les voies de communication empruntées par une requête DNS. Chaque résolveur est relié à chaque serveur faisant autorité de façon à leur communiquer toute requête DNS et à se voir communiquer la réponse à ladite requête. Les serveurs faisant autorité ne sont pas directement interreliés car ils ne se communiquent pas la requête DSN entre eux, mais ils sont indirectement tous interreliés par le biais du résolveur qui leur sert d'intermédiaire avec le terminal.

Dans cette modélisation minimale du réseau DNS, on a exposé : 22 résolveurs DNS dont dix-neuf publics et trois par défaut ; 10 registrars parmi les quinze qui stockent le plus grand nombre de noms de domaine dans le monde (GoDaddy, NameCheap, Tucows, Google, Network Solutions, IONOS, GMO Internet, Namesilo, OVH et Registrar of Domains REG.RU) ; 6 registries parmi les dix qui stockent les TLD les plus utilisés mondialement (<.com> géré par VeriSign, <.org> géré par Public Interest Registry sous la tutelle de l'Internet Society, <.ru> géré par le Coordination Center for TLD RU, <.de> géré par Denic, <.uk> géré par Nominet UK et <.in> géré par INRegistry) ; et un seul serveur racine (le serveur racine A)⁹⁹¹. D'abord, soulignons que le réseau DNS est nettement plus vaste que représenté ici. Il n'existe pas 22 résolveurs, mais l'Icann en dénombrait plus de 10 millions en 2012⁹⁹² (cela ne correspond évidemment pas au nombre de propriétaires de résolveurs DNS, que nous n'avons pas trouvé). Les registrars ne sont pas au nombre de 10 mais de 2567 dans le monde. Quant aux

⁹⁹¹ D'après la base de données *DomainNameStat.com* [en ligne], en 2022, GoDaddy enregistrait 76 729 014 noms de domaine, soit 12.31% de la totalité des noms de domaine enregistrés dans le monde. Le deuxième registrar par le nombre de noms de domaines enregistrés, NameCheap, en comptait 16 178 310 soit 2.69% de la totalité des noms de domaine enregistrés dans le monde. Les 10 principaux registrars représentent 23.3% de la totalité des noms de domaine enregistrés mondialement, et les 76.6% restants se partagent entre les 2557 autres registrars. D'après la base de données w3Tech, en septembre 2022, sur 52.2% de la totalité des sites web, le 4.1% des noms de domaine dans le monde étaient enregistrés en <.ru>, 1.9% en <.uk>, 1.8% en <.de>, 1.7% en <.in> et 1.4% en <.ir> : « Usage statistics of top level domains for websites » sur W3Techs.com

⁹⁹² ABLEY Joe, « Ten Million DNS Resolvers on the Internet », *Icann.org*, mars 2012

registries, on en compte plus de 900 différents qui gèrent 1 591 TLD⁹⁹³. Enfin, les serveurs racine sont au nombre de 13 (de A à M), tous gérés sous l'autorité de l'Icann⁹⁹⁴. Les serveurs racine B à M sont des répliques du serveur racine A. Sept serveurs racine sont situés exclusivement aux États-Unis, les six autres serveurs racine sont disséminés sur les territoires de 42 pays, y compris les États-Unis. Cette échelle réelle du réseau DNS (dizaine(s) de millions de résolveurs, milliers de registrars, centaines de registries, treize serveurs racine) ne modifie pas la structure réseau minimale proposée, mais en démultiplie seulement le nombre de nœuds verts, bleus, jaunes et rouges. Ensuite, ajoutons que les résolveurs DNS publics sont volontairement sur-représentés dans notre schéma par rapport aux résolveurs DNS par défaut, ceci dans le but de montrer la diversité des résolveurs DNS publics.

À l'image de son mode de gestion, on remarque que la centralisation est là encore hybride. D'un côté, toute requête DNS doit nécessairement emprunter l'un des treize serveurs racine, de sorte qu'il n'existe dans le monde entier que 13 voies d'accès à la totalité des TLD. Surtout, ces treize voies d'accès relèvent exclusivement d'un seul gestionnaire privé – l'Icann – et le territoire états-unien qui concentre plus de la moitié des serveurs racine en plus d'être le seul territoire accueillant tous les serveurs constitutifs d'un serveur racine au moins. Cette dépendance de toute requête DNS aux serveurs racine reflète une forte centralisation de la validité des requêtes d'accès à seulement 13 voies d'accès. Il suffit donc qu'un seul acteur – l'Icann – restreigne l'accès à un ou plusieurs TLD pour que ces TLD soient inaccessibles dans le monde entier, pour que soit invalidée toute requête DNS d'accès à ce TLD. De même, une panne des 13 serveurs racine provoquée par une cyberattaque suffit à invalider toute requête DNS et ainsi à rendre internet mondialement inutilisable. Au surplus, tout nom de domaine découle fondamentalement d'un TLD, ce qui conduit certains chercheurs à constater la centralité de l'Icann pour la détermination de l'espace de nommage sur internet⁹⁹⁵.

D'un autre côté, le réseau DNS comporte d'importantes sources de décentralisation. Premièrement, le choix de conditionner l'accès au réseau DNS par des résolveurs a pour effet

993 On a obtenu ce chiffre en dénombrant les registries gestionnaires des différents TLD recensés par l'Iana sur sa base de données « Root Zone Database » (base de données de la zone racine) [en ligne sur iana.org]

994 Un serveur-racine ne désigne pas un serveur à proprement parler, mais un réseau de plusieurs serveurs géographiquement dispersés. Un service-racine se distingue par l'adresse IP publique de son réseau de serveurs, de façon que les 13 serveurs-racines désignent en fait 13 adresses IP interrogeables par le résolveur. Par ex., le serveur racine J est constitué de serveurs situés en Irlande, au Royaume-Uni, au Luxembourg, en Corée du Sud, au Japon, en Malaisie, en Thaïlande, au Canada, aux États-Unis, au Brésil en Suède et en Australie

995 Aurélien Bamdè, l'un des principaux partisans de l'explication d'une gestion centralisée des noms de domaine, p. 369 : « un domaine étant constitué d'une zone [TLD] et de toutes les zones qui lui sont inférieures [successivement ccTLD, gTLD, nom de troisième niveau, SLD], l'espace de nommage put être étendu à l'infini. Plus un domaine est proche de la racine, plus l'espace de nommage qui lui est attaché est grand. Le domaine de la racine constitue donc l'intégralité de l'espace de nommage alors qu'un domaine de deuxième niveau n'en constitue qu'une petite fraction. (...) Alors que les pères fondateurs du DNS ont trouvé là, dans son architecture décentralisée, un formidable moyen d'endiguer la rareté des noms de domaine, assez paradoxalement, ils viennent corrélativement déposséder les internautes du pouvoir de gouvernance qu'ils exerçaient jusque-là, en commun, sur l'espace de nommage. Dorénavant, celui-ci est entièrement géré par ceux qui disposent de la maîtrise de la racine. ». V. aussi BRICTEUX Caroline, *Régulation de l'Internet par les noms de domaine. Le régime juridique et institutionnel de l'ICANN*, Thèse de droit, Université libre de Bruxelles, 2021, p. 32s.

de diversifier les voies d'accès à ce réseau. L'extrémité du réseau DNS se diversifie à mesure qu'augmente le nombre de voies d'accès et de leurs gestionnaires. Or, on a relevé que les voies d'accès fournies par les résolveurs sont très nombreuses (plus de 10 millions), tout comme leurs gestionnaires. Dans tous les pays connectés à internet, chaque FAI de grande voire de moyenne taille fournit plusieurs résolveurs DNS par défaut. Au-delà même des résolveurs par défaut, le marché des résolveurs publics n'a cessé de s'élargir depuis l'apparition du réseau internet. Les voies d'accès au réseau DNS ne sont donc pas limitées aux 13 fournies par les racines, mais aux plus de 10 millions de voies gérées par plusieurs milliers de gestionnaires dans le monde. Jouant le rôle d'interface entre l'utilisateur et le réseau DNS dont il fait partie, le résolveur est l'outil principal pour décentraliser l'accès à ce réseau, car c'est précisément de cet outil que dépend cet accès.

Deuxièmement, le choix de constituer une racine par un réseau de serveurs dispersés a pour effet de diversifier les voies d'accès aux racines. Les serveurs membres du réseau d'une racine sont interconnectés en *anycast* (chaque membre du réseau *anycast* est connecté à plusieurs autres membres du réseau déterminés), par opposition à l'interconnexion en *unicast* (chaque membre du réseau *unicast* n'est connecté qu'à un autre membre du réseau) ou en *broadcast* (chaque membre du réseau *broadcast* est connecté à tous les autres membres du réseau). De cette façon, si le serveur français constitutif de la racine F tombe en panne, les 38 autres serveurs constitutifs de la racine F prendront le relai. Le nombre de voies d'accès au serveur F ne sera alors plus de 39 mais de 38. Le réseau *anycast* des racines semble les préserver efficacement des cyberattaques. Trois importantes attaques par déni de service (DDoS, saturant les serveurs par un envoi excessif de requêtes depuis des machines infectées) ont été dirigées contre les racines en 2002 (100-200 000 requêtes/seconde), en 2007 et en 2015 (5 millions requêtes/seconde), sachant que l'attaque de 2007 a perturbé quatre racines et que les attaques de 2002 et 2015 ont affecté les treize racines. Grâce au relai assuré par l'*anycast*, aucune de ces attaques n'a eu d'incidence majeure sur l'accès aux noms de domaine. En d'autres termes, la décentralisation par *anycast* des serveurs constitutifs des racines permet de diversifier les voies d'accès aux racines pour sécuriser leur accessibilité.

Troisièmement, le choix de morceler les noms de domaines a pour effet de diversifier la gestion des noms de domaine à travers le réseau DNS. La gestion des domaines se diversifie à mesure qu'augmentent le nombre de sources de dépendances d'un nom de domaine et le nombre de gestionnaires des domaines. D'abord, le morcellement diversifie les sources de dépendances d'un nom de domaine : une pluralité de serveurs faisant autorité se partage les tronçons d'un même nom de domaine, ce qui signifie qu'**aucun nom de domaine ne dépend d'un seul serveur faisant autorité**. Cette indépendance des domaines à toute gestion exclusive par un seul serveur faisant autorité implique, comme le fait remarquer S. Bortzmeyer, qu'« *un serveur faisant autorité ne fait pas autorité pour tous les noms de domaine, puisque le DNS est décentralisé* »⁹⁹⁶. Cette indépendance implique aussi qu'un même nom de domaine n'obéit pas nécessairement à deux (racine et registrar) voire trois (registry) serveurs différents faisant autorité, mais peut obéir à une plus grande diversité de serveurs faisant autorité sur lui s'il est stocké par plusieurs registrars – tel que le domaine <sante.gouv.fr> sur lequel 6 serveurs différents font autorité⁹⁹⁷. En plus de diversifier les sources de dépendance d'un domaine, le morcellement diversifie les gestionnaires d'un même domaine. On a vu d'abord que les serveurs faisant

996BORTZMEYER S., « Serveur DNS faisant autorité : définition », préc., 2020

997Ibid.

autorité sont gérés par trois types d'acteurs différents (Icann, registries et registrars). On a vu ensuite que le stockage des TLD dont l'Icann délègue la gestion est géré par plus de 900 registries différents, et que l'enregistrement des domaines est géré par plus de 2560 registrars différents – attendu que plus de 90% des registries et registrars sont des acteurs privés⁹⁹⁸. Par conséquent, doit être très largement relativisée l'idée selon laquelle l'Icann pourrait dans les faits exercer sur les noms de domaine un pouvoir de gestion exclusive et autosuffisante.

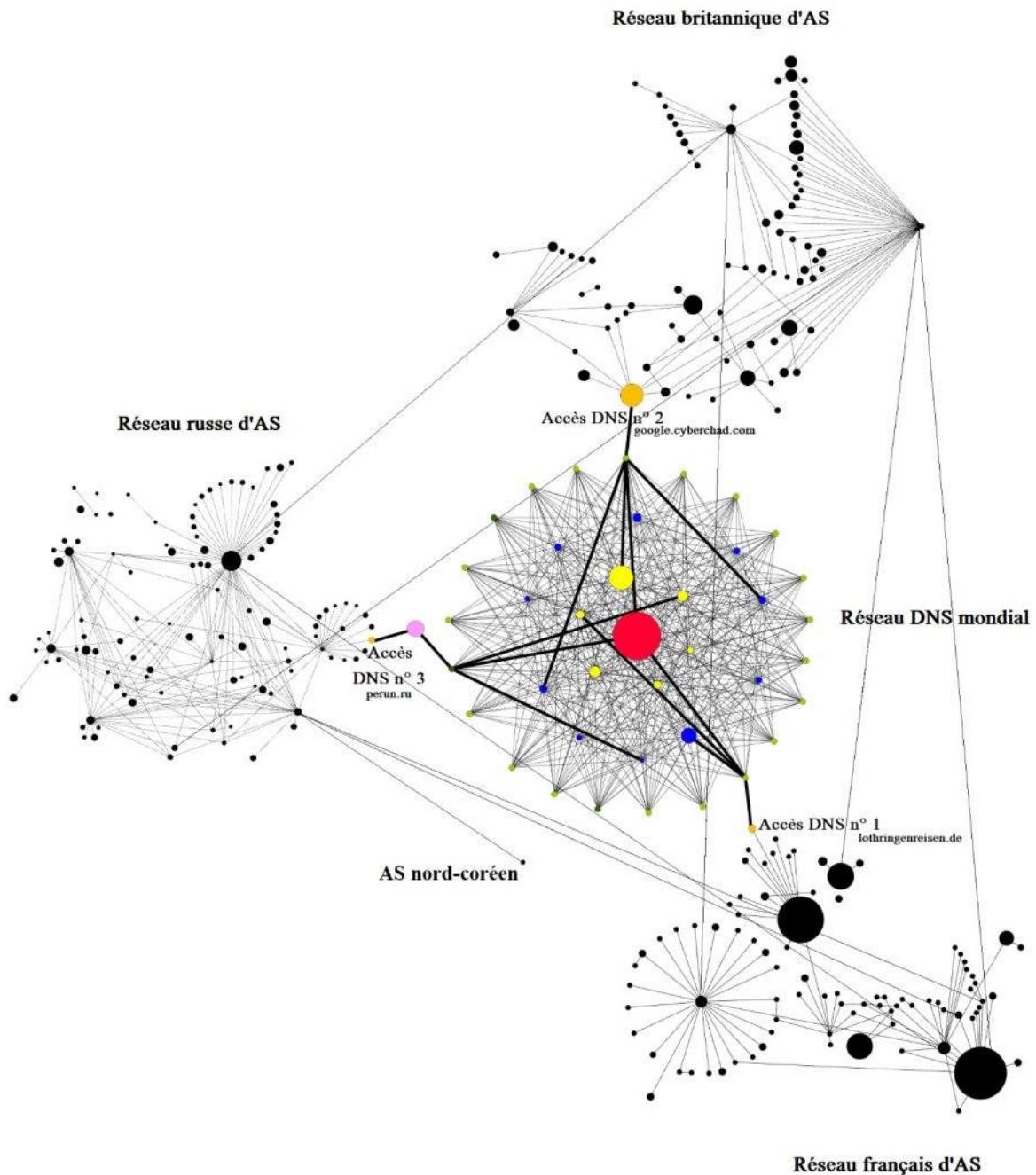
La décentralisation par les résolveurs, par l'interconnexion anycast des serveurs racine et par le morcellement de la gestion des noms de domaine contrebalance la centralisation due à la fondamentalité des racines, à leur faible nombre et à l'exclusivité de leur gestionnaire (l'Icann). En somme, la centralisation hybride du réseau DNS se traduit par une ossature centralisée (racines) sur laquelle est superposée une structure réseau décentralisée par des serveurs faisant autorité qui dépendent contractuellement de l'Icann (registries et registrars) et par des résolveurs qui ne dépendent ni de l'Icann, ni des serveurs faisant autorité. Métaphoriquement, le réseau DNS s'apparente à un royaume, dans lequel une Reine (l'Icann) exerce l'autorité (technique et contractuelle) sur une Administration décentralisée (registries et registrars), et dont les voies d'accès aux services royaux seraient fournies par des acteurs indépendants du Royaume et diversifiés ; si la Reine désire se débarrasser de l'une de ses administrations, elle en a techniquement et contractuellement le pouvoir mais ces administrations gèrent en principe librement la prestation des services royaux sur délégation de la Reine ; si la Reine excède sa neutralité ou intensifie sa centralité, elle court cependant le risque que soit mise en cause sa légitimité voire son existence. Sous cet angle, la gouvernance du DNS ressemble à une monarchie de type britannique.

B) Naissance d'un National DNS (NDNS) : la centralisation russe de l'accès aux noms de domaine

Comment les réseaux nationaux accèdent-ils au réseau DNS mondial ? Toute requête DNS émise depuis un réseau national est acheminée jusqu'au réseau DNS. On le représente ainsi :

⁹⁹⁸On a évalué ce pourcentage à partir de la *Root Zone Database* fournie par l'IANA. Le registry russe gestionnaire du <.ru> est un acteur privé, mais pas le registry chinois gestionnaire du <.cn>, le China Internet Network Information Center (CNNIC), une organisation étatique sous la tutelle du ministère chinois de l'Industrie et des Technologies de l'information.

Interconnexion des réseaux nationaux d'AS avec le réseau DNS mondial



Ce schéma reproduit les réseaux d'AS précédemment établis. On y a précisé certains liens de *peering* entre les AS russes (Rostelecom, Yandex et TTK), britanniques (Colt et RTN Limited) et français (Renater, Orange, Céleste et Adista) – les fameux « AS étrangers » auxquels sont connectés les AS des réseaux nationaux – de façon à représenter quelques principales interconnexions de ces trois réseaux nationaux. On a séparé le réseau DNS de l'ensemble des AS pour faciliter la lecture du schéma, mais les serveurs DNS – comme toute machine connectée à internet – sont des membres des AS et se situent donc à l'intérieur d'un AS.

Cette modélisation retrace le parcours de trois requêtes DNS. La première (« Accès DNS n° 1 ») est transmise au résolveur public UncensoredDNS depuis le réseau français – particulièrement depuis les routeurs constitutifs de l’AS de Moselle Telecom qu’on a coloré en orange. Le résolveur interroge successivement la racine (nécessairement), le serveur du registry Denic gestionnaire du point <.de> et le serveur du registrar GoDaddy. Cela signifie qu’un utilisateur accède à un nom de domaine enregistré par GoDaddy et s’achevant par le TLD <.de> (ex. fictif : <lothringenreisen.de>), grâce au résolveur public UncensoredDNS qui se voit transmettre la requête DNS par l’opérateur français Moselle Telecom. La deuxième requête DNS (Accès DNS n° 2) envisage une configuration différente. Le site internet ici accédé s’achève par le TLD <.com>, débute par le sous-domaine <google.> mais son SLD est enregistré par Tucows (ex. fictif : <google.cyberchad.com>). Le nom de domaine dépend donc de quatre serveurs faisant autorité : la racine gérée par l’Icann ; le serveur du registry VeriSign gestionnaire du <.com> ; le serveur du registrar Google gestionnaire du sous-domaine <google.> ; et le serveur du registrar Tucows gestionnaire du nom de domaine <google.cyberchad.com>. En l’espèce, la requête DNS de l’utilisateur est transmise au résolveur public Cloudflare depuis le réseau britannique – en particulier par les routeurs constitutifs de l’AS2856 de BT –, et la réponse à la requête dépend des serveurs de l’Icann, de VeriSign, de Google et de Tucows.

La troisième requête DNS (Accès DNS n°3) est encore différente des deux précédentes. Provenant du réseau russe, elle est transmise par l’AS41733 d’ER-Telecom à un résolveur par défaut d’ER-Telecom. En l’espèce, la requête demande l’accès à un nom de domaine s’achevant par le TLD <.ru> (géré par l’autorité privée Coordination Center for TLD RU) et enregistré sur les serveurs du registrar privé Registrar of Domain Names REG.RU (par ex. fictif : <perun.ru>). Assez classiquement, elle dépend donc d’une racine de l’Icann, d’un registry et d’un registrar privés. Cependant, une anomalie s’observe : un nœud rose s’intercale entre l’AS d’ER-Telecom et son résolveur par défaut. Cette anomalie est le fruit de la loi russe de 2019 sur l’internet souverain.

La loi de 2019 annonce la naissance de RuNet, un réseau internet russe qui se veut autonome de l’étranger et autosuffisant nationalement. RuNet repose sur trois piliers techniques : les AS ; l’instauration d’un « système national de nom de domaine » (*National Domain Name System*, NDNS)⁹⁹⁹ ; et la *deep packet inspection* (DPI). La loi s’appuie sur le premier pilier pour confier au Roskomnadzor le pouvoir et la responsabilité de superviser l’acheminement sur le réseau russe¹⁰⁰⁰. La législation s’inspire d’abord du modèle chinois en scindant les voies d’accès nationales et internationales du réseau : tout propriétaire ou détenteur d’AS désireux de se relier à un AS étranger doit respecter « les modalités, la procédure, la présentation et le format déterminés par » le Roskomnadzor, et informer ce dernier sur « les buts de l’exploitation de la ligne [internationale] et les moyens de communication installés sur ladite ligne » ainsi que sur les lieux où se connectent et où sont installés ses moyens de communication avec des lignes internationales¹⁰⁰¹. Outre cette centralisation de la gestion des voies internationales d’accès par le Roskomnadzor, les dispositions organisent ensuite tout un système de centralisation des voies nationales d’accès. Tout d’abord, le Roskomnadzor établit un « registre des points d’échange de trafic », un répertoire dans lequel il recense les points d’échange (IXP *i.e.* les liens de *peering*)

⁹⁹⁹ Loi sur l’information de 2006, art. 14.2 issu de l’art. 2 de la loi n° 90 FZ pour un internet souverain

¹⁰⁰⁰ Loi n° 126 FZ sur les communications de 2003, art. 56.1 issu de l’art. 1^{er} de la loi pour un internet souverain

¹⁰⁰¹ *Ibid.*, art. 56.2, §1 et art. 56.2, §8, 4

dont il autorise l'exploitation par les propriétaires et détenteurs d'AS. Ensuite, les « *propriétaires ou détenteurs de numéros d'AS* » doivent « *utiliser les points d'échange de trafic figurant dans le registre [du Roskomnadzor] pour transmettre des communications* »¹⁰⁰². De plus, tout propriétaire ou détenteur d'AS sur le sol russe doit communiquer au Roskomnadzor les informations relatives au numéro et aux adresses IP de l'AS dont il dispose, aux interactions avec tout autre propriétaire d'AS, aux itinéraires des messages de télécommunication, à l'infrastructure de son réseau et à la technologie DPI utilisée¹⁰⁰³. Enfin, il est fait interdiction aux propriétaires ou détenteurs d'AS d'établir un lien de peering avec des AS dont les propriétaires ou détenteurs refusent d'installer une technologie DPI, refusent de coopérer ou d'assister le Roskomnadzor et les services d'enquête et de sécurité de la Fédération, ou permettent la transmission de « *ressources d'information (site internet, page internet, système d'information, programme informatique) (...) dont l'accès est restreint* » d'après une liste du Roskomnadzor¹⁰⁰⁴. Concrètement, ces dispositions donnent au Roskomnadzor un pouvoir d'architecte du réseau russe de l'acheminement, lui offrant de remodeler totalement la cartographie du réseau national d'AS selon les schémas de routage arrêtés par le Roskomnadzor, de redéfinir les liens entre les AS nationaux et avec des AS étrangers, de centraliser les points d'échange de trafic et donc les voies d'accès du réseau national, et d'isoler les AS insubordonnés à la loi de tout lien d'échange avec un AS national ou étranger.

Le deuxième pilier de RuNet a pour objet de centraliser non l'acheminement mais l'accès aux noms de domaine depuis la Russie. Pour ce faire, la loi crée une racine DNS russe : elle prévoit la réplication du contenu des racines de l'Icann sur des serveurs nationaux ; comme les racines de l'Icann, ces serveurs nationaux sont connectés en anycast pour sécuriser l'accès aux noms de domaine ; constitutifs de la racine DNS russe, ces serveurs dispersés en Russie sont placés sous la propriété et la gestion du Roskomnadzor¹⁰⁰⁵. Le troisième pilier technique sur lequel repose RuNet – la DPI – fait de la centralisation de l'acheminement et de l'accès DNS un outil au service de la politique de restriction d'accès du Roskomnadzor (blocage, filtrage...). D'abord, tout propriétaire ou détenteur d'AS doit « *veiller à installer, dans son réseau de communication, des moyens techniques contrôlant le respect par [ces propriétaires ou détenteur] des exigences des lois* » de 2003 sur les communications (dont l'art. 15.8 fonde la liste du Roskomnadzor des ressources d'information à censurer) et de 2006 sur l'information (dont l'art. 15.1 fonde le registre du Roskomnadzor des contenus et services à censurer)¹⁰⁰⁶. La loi pose ainsi l'obligation de recourir à la DPI à des fins de filtrage des ressources d'information, services et contenus illicites listés par le Roskomnadzor ainsi que des « *menaces à la stabilité, à la sécurité et à l'intégrité (...) du réseau public de communication sur le territoire de la Fédération* »¹⁰⁰⁷. Ensuite, les opérateurs doivent employer la DPI pour analyser les paquets IP (notamment leur provenance) et les retransmettre vers les points d'échange figurant dans le registre du Roskomnadzor¹⁰⁰⁸. Enfin, ils doivent employer la DPI pour retransmettre les paquets IP russes vers les serveurs DNS

¹⁰⁰² *Ibid.*, art. 56.2, §3 pour le registre et art. 56.2, §8, al. 2 pour le devoir des opérateurs de suivre le registre

¹⁰⁰³ *Ibid.*, art. 56.2, §8, al. 4

¹⁰⁰⁴ *Ibid.*, art. 56.2, §9

¹⁰⁰⁵ Loi sur l'information de 2006, art. 14.2 issu de l'art. 2 de la loi pour un internet souverain

¹⁰⁰⁶ Loi sur les communications de 2003, art. 56.2, §9, al. 2 issu de l'art. 1^{er} de la loi pour un internet souverain

¹⁰⁰⁷ *Ibid.*, art. 46, §5.1

¹⁰⁰⁸ *Ibid.*, art. 56.2, §8, al. 2

constitutifs de la racine russe, et le Roskomnadzor assure la poursuite du trafic à travers son serveur racine¹⁰⁰⁹. De cette façon, **tous les opérateurs membres du réseau national russe doivent transférer le trafic DNC vers la racine DNS (« racine-clone ») du Roskomnadzor.**

Sur le schéma représentant l'interconnexion des réseaux nationaux d'AS avec le réseau DNS mondial, le nœud rose, l'« anomalie » que nous évoquions représente la racine-clone du Roskomnadzor. Comme tout propriétaire d'AS en Russie, ER-Telecom est contraint de rediriger la requête DNS vers la racine-clone du Roskomnadzor. Grâce à la copie des racines de l'Icann, la racine-clone peut « *obtenir des informations sur les adresses IP et les noms de domaine* »¹⁰¹⁰, et s'appuyer sur ces informations pour reprendre le trafic en envoyant la requête DNS au résolveur destinataire mentionné dans l'en-tête de la requête. En faisant écran entre le réseau national d'AS et le réseau DNS mondial, **le NDNS russe permet au Roskomnadzor de bloquer et/ou de filtrer l'accès à n'importe quel nom de domaine stocké sur le réseau DNS mondial depuis n'importe quel AS fournisseur de services de routage en Russie**¹⁰¹¹.

Dès son adoption en 2003, la loi sur les communications prévoyait un régime d'état d'urgence pour internet à travers son chapitre 10 « Gestion des réseaux de communication dans les situations d'urgence » : « *dans les situations d'urgence, la gestion du réseau public de communication est assurée par le [Roskomnadzor]* »¹⁰¹². La loi de 2019 en offre désormais les moyens au Roskomnadzor. Elle insère un nouvel art. 65.1 dans le Chapitre 10, qui reconnaît au gouvernement la prérogative de déclarer l'état d'urgence numérique, qui conditionne cette déclaration par l'existence de « *menaces à la stabilité, à la sécurité et à l'intégrité du fonctionnement du réseau public de communication sur le territoire fédéral* », et qui attribue à cet état d'urgence la conséquence de déclencher une « *gestion centralisée du réseau public de communication* »¹⁰¹³. La « gestion centralisée » intervenant en état d'urgence s'effectue au moyen de la DPI, et consiste pour le Roskomnadzor à surveiller le fonctionnement du réseau et à définir des « *règles d'acheminement des messages de télécommunications* » que doivent respecter « *les personnes participant à la gestion centralisée* »¹⁰¹⁴. En pratique, cet état d'urgence opère donc grâce à l'établissement par le Roskomnadzor de schémas de routage spécifiques à l'urgence, destinés à couper l'accès du réseau russe de l'acheminement à des sources (AS national, AS étranger, nom de domaine) porteuses de menaces à la stabilité, la sécurité ou l'intégrité dudit réseau. Ce régime d'exception prétend donner à l'État fédéral le pouvoir de

¹⁰⁰⁹ *Ibid.*, art. 56.2, §8, al. 3

¹⁰¹⁰ Loi sur l'information de 2006, art. 14.2, §1

¹⁰¹¹ *Ibid.*, art. 15.1-1, §10, art.15.3, §7.1, art. 15.5, §10.1 et art.15.8, §15.1 issus de l'art. 2 de la loi pour un internet souverain

¹⁰¹² Loi sur les communications de 2003, art. 65. Précisons que, selon la loi constitutionnelle fédérale n° 3-FKZ du 30 mai 2001 relative à l'état d'urgence, l'état d'urgence ne peut être déclaré qu'en présence de circonstances qui constituent une menace directe pour la vie et la sécurité des citoyens ou pour l'ordre constitutionnel fédéral.

¹⁰¹³ *Ibid.*, art. 65.1, al. 5 (motifs de déclaration de l'état d'urgence) et 2 (gestion centralisée du réseau)

¹⁰¹⁴ *Ibid.*, al. 4 et 6

déconnecter le réseau internet russe de tout réseau étranger¹⁰¹⁵, bien que ce régime soit inappliqué et surtout inapplicable à ce jour¹⁰¹⁶.

Sur le plan des techniques de régulation, on tire deux leçons de l'échec russe à uniformiser le filtrage. D'une part, cet échec confirme ce que nous avons démontré logiquement, à savoir que la lourdeur économique et technique et du filtrage rend cette technique inefficace faute d'un réseau national d'acheminement suffisamment centralisé ou de moyens financiers étatiques suffisants. Par contraste, la centralisation chinoise permet de faire reposer le filtrage et le blocage de l'ensemble du réseau d'acheminement sur un très petit nombre d'opérateurs (principalement China Telecom, China Unicom, China Mobile, le Ministère de l'Éducation, Tencent, NetEase et 21Viannet), et les investissements publics conséquents apportés aux principaux opérateurs (China Telecom, China Unicom, China Mobile et le Ministère de l'Éducation) leur donne la capacité de soutenir financièrement la technologie de filtrage. Les petits opérateurs n'ont pas à supporter les coûts du filtrage car le trafic national dépend entièrement des grands opérateurs. On confirme donc, en pratique, que **la lourdeur économique et technique du filtrage peut être compensée par une centralisation de l'acheminement et/ou des moyens financiers étatiques suffisants**. On rappelle que la centralisation permet par ailleurs de relativiser le deuxième gros inconvénient du filtrage – la facilité de son contournement. Par la centralisation de son réseau national

¹⁰¹⁵ Lors d'une conférence de presse le 1^{er} février 2021, le président du Conseil de Sécurité de Russie – Dmitri Medvedev – a soutenu que « *technologiquement, tout est prêt* » pour déconnecter le réseau russe de l'internet mondial (« Pourquoi les autorités veulent-elles créer un "RuNet souverain" : de quoi protège-il contre quelles menaces ? » (Зачем власти создают «суверенный Рунет»: от чего он защитит и чем грозит), sur *Trends.rbc.ru*, mis à jour le 28 fév. 2022).

¹⁰¹⁶ Le réseau russe ne saurait être centralisé en octobre 2022, RuNet est encore en construction. En décembre 2019, conformément à l'art. 56.1, §3 de la loi sur les communications de 2003, plusieurs essais de RuNet ont été menés par Rostelecom, TTK, Tele2, MegaFon, VimpelCom, MTS, Modern Radio Technologies, Group IB, Positive Technologies et Kaspersky Lab. Le ministère des Communications et des Médias a prétendu un succès. Toutefois, la majorité des opérateurs n'ayant pas les moyens financiers de se procurer une technologie DPI, le gouvernement a dû, en février 2020, reporter sur l'État la charge de payer les mises à niveau des équipements DPI lorsque la DPI ralentit la qualité ou la vitesse de connexion (« L'équipement du "RuNet souverain" sera modernisé aux frais de l'État » (Оборудование для "суверенного рунета" модернизируют за счет государства) [en ligne], *Kommersant*, 17. fév. 2020). En mars 2020, le ministère des Communications et des Médias a reporté les exercices prévus pour RuNet en raison de la pandémie de Covid-19. En septembre 2020, le ministère des Communications et des Médias annule une troisième fois les exercices au motif qu'« *il y a une révision active du projet fédéral [sur l'internet souverain] et des actes réglementaires dans le domaine* » – comprendre que les essais n'ont pas été concluants et nécessitent de corriger la régulation établie (« Le ministère des communications a une nouvelle fois annulé l'exercice dans le cadre de la loi sur le RuNet souverain » (Минцифры вновь отменило учения в рамках закона о суверенном Рунете) [en ligne], *Interfax*, 21 sept. 2020). En avril 2021, MTS, MegaFon, Tele2, VimpelCom et le grand opérateur régional Obit ont déclaré que la DPI faisait échouer la transmission des paquets, les obligeant à abandonner la technologie pour reprendre le trafic (« Échecs pour l'indépendance. Le trafic se perd dans les équipements du "Runet souverain" » (Сбои за независимость. В оборудовании «суверенного рунета» заблудился трафик) [en ligne], *Kommersant*, 9 avr. 2021). En janvier 2022, le Roskomnadzor adopte une ordonnance qui transfère aux opérateurs la gestion des données relatives au trafic des abonnés. Le Roskomnadzor transfère ainsi certaines de ses tâches aux acteurs du marché, faisant peser sur ce derniers une dépense excessive pour la gestion du volume des données de trafic, que la plupart d'entre eux peuvent pas assumer selon le ministère de l'Économie (« Le RuNet souverain en cours de retrait de la circulation. Le ministère de l'économie s'oppose aux nouvelles idées du Roskomnadzor » (Суверенный рунет выбивается из трафика. Минэкономики против новых идей Роскомнадзора) [en ligne], *Kommersant*, 20 fév. 2022).

d'acheminement et par ses investissements, l'État en Chine relativise considérablement les inconvénients du filtrage pour en tirer les meilleurs avantages, et s'est ainsi toujours épargné l'inefficacité du filtrage qui touche la Russie.

D'autre part, la centralisation par le Roskomnadzor d'un système national de nom de domaines engendre l'institution d'un « *point unique de défaillance* » comme le dénonçait la Commission des technologies de la communication, de l'information et des télécommunications de l'Union russe des industriels et des entrepreneurs (RSPP) ¹⁰¹⁷. La directrice des projets stratégiques à l'Institut de recherche sur Internet, Irina Levova, abondait en ce sens, soulignant que le fonctionnement d'internet en Russie pourrait être paralysé s'il était mis entre les mains du Roskomnadzor ¹⁰¹⁸. Il suffit qu'un seul agent du Roskomnadzor commette une erreur ou qu'une seule cyberattaque soit téléchargée sur les serveurs du Roskomnadzor pour que l'internet russe s'effondre, *i.e.* pour que le trafic national ne puisse plus accéder au moindre nom de domaine internet (et donc à la quasi-totalité des services russes en ligne). Le risque pris par la Fédération avec l'instauration d'un NDNS centralisé est colossal pour l'économie russe, dès lors qu'un **accident affectant une seule administration** peut empêcher toute entreprise russe de fournir des services en ligne et tout consommateur russe d'y accéder – en somme, **peut empêcher tout commerce en ligne sur le réseau russe**. Comme on l'avait déjà observé pour la Corée du Nord dont le réseau internet s'était effondré sous l'effet d'une seule cyberattaque, **on confirme donc la causalité entre centralisation et vulnérabilité d'un réseau**. À nouveau, la Chine parvient à nuancer fortement cet inconvénient de la vulnérabilité en décentralisant son réseau *a minima* : contrairement au NDNS russe ou à l'AS nord-coréen, aucun nœud ne sert de voie unique d'accès dans le réseau national. Que ce soit pour accéder au réseau DNS mondial, à un autre réseau étranger, ou à un réseau membre du réseau national, les nœuds du réseau chinois de transmission offrent toujours plusieurs voies d'accès.

En somme, le Runet souverain fait aujourd'hui preuve non seulement d'inefficacité mais surtout de contre-productivité – trop coûteux pour l'État et les opérateurs, manquant d'uniformité et suscitant des problèmes d'acheminement du trafic le rendant incapable de tout isolement aujourd'hui, créant un risque démesuré pour l'économie et le réseau internet russes. Outre le NDNS russe, on a aussi représenté l'AS nord-coréen sur notre schéma. Cet AS est relié à celui de TTK en Russie, comme on l'a vu plus haut. La centralisation DNS en Corée du Nord s'effectue à deux niveaux : la gestion du TLD <.kp> ; l'accès au réseau DNS mondial. Concernant la gestion du TLD <.kp>, elle est assurée depuis 2011 par Star JV après un transfert de compétences de la part de KCC Europe dont le mandat pour la gestion du <.kp> venait d'expirer¹⁰¹⁹. Depuis 2011, le <.kp> est donc géré sur le territoire nord-coréen et non plus allemand. Concernant l'accès au réseau DNS mondial, le fait que le réseau internet nord-coréen soit constitué par un seul AS implique que ce réseau offre par l'acheminement une seule voie

¹⁰¹⁷ TISHINA Julia, « Runet Souverain est hors lige » (Суверенный рунет вышел на связь), *Kommersant.ru*, 8 février 2019

¹⁰¹⁸ BALASHOVA Anna, KUZNETSOVA Evgeniya, POSYPKINA Alexandra, « La Russie, rien que la Russie : quels sont les risques du projet sur le Runet souverain? » (РФ и точка: какие риски несет проект о суверенном Рунете) [en ligne], *RBC*, 15 déc. 2018

¹⁰¹⁹ SELIGER Bernhard et SCHMIDT Stefan, « The Hermit Kingdom Goes Online ... Information Technology, Internet Use and Communication Policy in North Korea », *North Korean Review*, vol. 10, 2014, p. 71-88

d'accès au réseau DNS mondial. Il est donc aisé, comme en Russie, d'y empêcher l'accès à toute requête DNS par blocage ou filtrage. L'instauration d'un NDNS ou la structuration du réseau d'acheminement par un seul AS sont deux méthodes différentes (centralisation du stockage des noms de domaines et centralisation de l'acheminement par le réseau IP) qui permettent respectivement à la Russie et à la Corée du Nord de recentraliser nationalement l'accès au réseau mondial des noms de domaine. Alors que le réseau DNS mondial ne relève de la compétence d'aucun État, la Russie et la Corée du Nord parviennent à neutraliser leur incompétence à cet égard par la technique de la centralisation (du stockage ou de l'acheminement) mais, dans les deux cas, cette « victoire » de la compétence étatique aggrave très fortement la vulnérabilité du réseau voire de l'économie – *a fortiori* lorsqu'échouent les techniques accompagnant la centralisation (filtrage, blocage, ralentissement).

Section 2. La centralisation dès le stockage des usages en ligne

On évaluera d'abord la centralité des applications à partir du nombre de connexions qu'elles concentrent (Paragraphe 1), puis on traitera leur centralité au regard de leur fonctionnement et de leur gestion (Paragraphe 2).

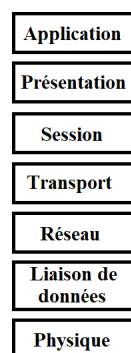
Paragraphe 1 – La centralité de connexion des applications

Après avoir mentionné les critères ici utilisés pour mesurer la centralité de connexion d'une application (A), on constatera qu'une application peut devenir centrale sur le plan des connexions dans trois situations au moins : lorsque l'application est à la fois novatrice et fédératrice (B), lorsqu'elle s'insère à une autre application centrale et lorsque des circonstances exceptionnelles la rendent centrale (C).

A) Évaluation de la centralité d'une application

Parmi les services stockés sur internet, lesquels sont les plus centraux ? On recense au total

deux types de services sur internet : les services qui permettent la communication entre la couche 7 Application du TCP/IP et les autres couches de ce protocole (qu'on appellera « services d'interopérabilité protocolaire ») ; et les services qui fournissent le contenu de la couche Application (qu'on appellera « services applicatifs »). Concernant les services d'interopérabilité protocolaire, on a déjà vu que le service DNS permet de rendre interopérable la couche 3 Réseau (adresses IP) avec la couche Application (services hébergés en ligne) au moyen des noms de domaine. Parmi les autres services d'interopérabilité protocolaire, le service DHCP (*Dynamic Host Configuration Protocol*) attribue aux différentes machines non leurs noms de domaine mais leurs adresses IP¹⁰²⁰. Ce service permet ainsi de rendre interopérable la



Modèle OSI (selon le standard de l'ISO) des couches, abrégées "TCP/IP"

¹⁰²⁰ Les adresses IP sont automatiquement attribuées à une machine par des serveurs DHCP. Pour en comprendre le fonctionnement, toute machine possède un système d'exploitation interopérable avec le protocole DHCP. Ce protocole permet de formuler des datagrammes DHCP, qui contiennent diverses informations. La machine dépourvue d'adresse IP adresse un datagramme DHCP (DHCP DISCOVERY) à un serveur DHCP ; le serveur DHCP y répond par un autre datagramme (DHCP OFFER) dans lequel il propose différentes adresses IP ; la machine cliente renvoie un nouveau datagramme au serveur DHCP pour l'informer de l'adresse IP qu'elle retient (celle qui lui parvient le

couche 3 Réseau (adresses IP) avec la couche Application (services hébergés en ligne).

En assurant l'interopérabilité de la couche Application avec les couches inférieures du TCP/IP, les services d'interopérabilité protocolaire (principalement DNS et DHCP) permettent l'accès aux applications en ligne. Outre les services d'interopérabilité protocolaire, les « applications en ligne », ou services applicatifs en ligne, sont le deuxième type de services internet. En sciences informatiques, le terme « **application** » désigne **tout logiciel autre que ceux nécessaires au fonctionnement de la machine**. Sont donc exclues de cette catégorie les systèmes d'exploitation (programmes qui offrent à l'utilisateur son environnement d'utilisation), certains *daemons* (programmes qui s'exécutent en arrière-plan sans intervention humaine, comme le *daemon* init du système d'exploitation Unix qui rend possible l'exécution de tout programme sur Unix), ou encore certaines tables de données installés dès la fabrication (programmes qui recensent les données nécessaires au fonctionnement de la machine, comme la table ASCII faisant correspondre chaque caractère ou symbole à une suite de bits pour convertir les signaux numériques en symboles représentés sur le clavier de la machine, la *Global Descriptor Table* qui définit et organise les capacités mémoire de la machine, l'*Interrupt Descriptor Table* qui permet d'organiser le traitement des informations en suivant un ordre de priorités...). Inversement, tous les logiciels non nécessaires au fonctionnement de la machine sont des applications. Lorsque l'accès à l'application n'exige pas de connexion internet, *i.e.* lorsque la seule utilisation du terminal qui l'héberge suffit pour accéder à cette application, on parlera d' « application locale » (certains éditeurs de texte comme Word, jeux vidéo hors-ligne, logiciels graphiques hors-ligne comme Photoshpe...); au contraire, lorsque l'accès à l'application se fait au moyen d'internet, *i.e.* par la transmission de la requête au serveur qui héberge cette application, on parlera d' « application en ligne » (sites web, navigateurs web, moteurs de recherche, jeux vidéo en ligne, réseaux sociaux, wikis¹⁰²¹...).

On définit donc l'**application en ligne** comme le **logiciel non nécessaire au fonctionnement du serveur qui l'héberge et accessible au moyen du réseau internet**. Dans le cadre de cette thèse spécialisée dans l'étude du réseau internet, on examinera seulement les applications en ligne, au détriment des applications locales. Telle que représentée dans le modèle TCP/IP, l'application en ligne recouvre la même réalité concrète que la définition qu'on vient de proposer. D'après ce modèle, la couche « application » et celle qui se situe au sommet, donc la dernière à laquelle parvient la requête de l'utilisateur. En ce sens, l'application en ligne désigne tout service accessible au moyen d'internet en-dehors des services d'interopérabilité protocolaire (situé dans les couches inférieures) et des services de fourniture d'accès à internet (situés dans la couche 3).

Que l'on soit en présence de services d'interopérabilité protocolaire, de services applicatifs ou d'opérateurs de transmission de données, on évalue la centralisation selon la même grille de

plus rapidement); enfin, le serveur DHCP communique au client un dernier datagramme DHCP qui contient la confirmation de l'adresse IP attribuée, le masque de sous-réseau correspondant, la durée du bail de l'adresse (bail renouvelable), voire des informations supplémentaires. Comme pour le réseau DNS, il existe un réseau DHCP composé des différents serveurs DHCP. V. ATELIN Philippe et DORDOIGNE José, *Réseaux informatiques*, Editions ENI, 2006, p. 116 et 350s., notamment le G (« Couche applicative TCP/IP ») du Chapitre 8 (« Protocoles des couches moyennes et hautes »)

¹⁰²¹ Un site web est une application en ligne qui offre la possibilité de produire et d'accéder à des hyperliens (*i.e.* qui propose des fonctionnalités issues du langage HTTP). Dès lors que les réseaux sociaux offrent cette fonction, ils sont qualifiables de sites web, que l'utilisateur y accède depuis son navigateur Web ou depuis l'application mobile qui lui sert de client pour communiquer avec le serveur. De même, un wiki est une application en ligne, généralement un site web, édité et géré en collaboration avec son public.

lecture que celle adoptée jusqu'à présent. Cette grille de lecture consiste à définir la centralisation comme une réduction de la diversité des voies d'accès empruntées ou empruntables, et à évaluer la centralité d'un nœud sous trois aspects : sa centralité de connexion (nombre de nœuds connectés par le nœud dont la centralité est évaluée) ; sa centralité de gestion (nombre de nœuds tiers ayant le même propriétaire que le nœud dont la centralité est évaluée) ; et sa centralité de fonctionnement (nombre de nœuds tiers qui assurent la même fonction que le nœud dont la centralité est évaluée).

Concernant le premier type de centralité, on s'intéresse ici à la centralité de connexion des applications. Comment mesurer la centralité de connexion d'une application ? On avait mesuré la centralité de connexion d'un AS selon le nombre d'adresses IP publiques qu'il connecte (*i.e.* qu'il attribue), car le rôle d'un AS dans la connexion internet consiste à connecter des adresses IP pour former un réseau IP cohérent. On a aussi mesuré la centralité de connexion d'un service de noms de domaine faisant autorité selon le nombre de noms de domaines qu'il connecte (*i.e.* qu'il héberge), car le rôle d'un tel serveur dans la connexion internet consiste à connecter des noms de domaines au réseau pour les y rendre accessibles. De même, le rôle d'une application dans la connexion du réseau internet consiste à connecter des utilisateurs à un service destinataire définitif : tout ce qui se trouve dans la couche application a vocation à être définitivement accédé par l'utilisateur. Pour cette raison, on mesurera la centralité de connexion d'une application selon le nombre d'utilisateurs qu'elle connecte. Précisément, on se reporte sur le nombre d'utilisateurs « actifs » que connecte une application. Fréquemment mobilisé en science marketing et en sociologie, le critère du nombre d'utilisateurs actifs d'une application décrit le nombre d'utilisateurs différents qui montrent des signes d'activité (par la régularité de leurs visites et de leurs connexions au service, la publication de contenus d'information, l'utilisation du produit...) sur une certaine durée¹⁰²². Cette métrique révèle le nombre d'utilisateurs humains qui peuvent

¹⁰²² La régularité de l'activité dans le temps est classiquement calculée à l'aide d'un ratio nombre d'Utilisateurs Actifs Mensuels (MAU) / nombre d'Utilisateurs Actifs Quotidiens (DAU), v. HUI Sam, « Understanding repeat playing behavior in casual games using a Bayesian data augmentation approach », *Quantitative Marketing and Economics*, vol. 15, 2017. Il est en marketing pour étudier les comportements des utilisateurs d'un service, la stabilité, l'influence et la cote de confiance d'un service auprès des investisseurs et des publicitaires, v. LEE Katherine, *Non-Financial Metrics, DAU, MAU, and DAU/MAU* [en ligne], Thèse en marketing, Université de Pensylvanie, Joseph Wharton Scholars, 2022. En sociologie, il est aussi employé pour étudier les comportements des utilisateurs par comparaison des actifs et des non-actifs, les types d'interactions qui se nouent entre utilisateurs et les cultures qui se forment sur un service, v. BASTARD Irène, CARDON Dominique, CHARBEY Raphaël, COINTET Jean-Philippe et PRIEUR Christophe, « Facebook, pour quoi faire ? », *Sociologie*, vol. 8, Presses Universitaires de France, 2017. D'autres critères peuvent venir compléter et préciser la centralité d'une application auprès des utilisateurs actifs, tel que le critère du « temps dépensé » sur une application ou du « temps d'attention » accordé par les utilisateurs à cette application. On retrouve ainsi souvent ces critères du temps dépensé ou du temps d'attention (critère de l'*attention span*) dans les sciences psychologiques pour jauger les impacts psychologiques des réseaux sociaux et des jeux vidéo sur les capacités d'attention des êtres humains et dans les sciences marketing pour optimiser les méthodes de captation de l'attention. En psychologie, v. par ex. CARSTENS Deborah, DOSS Samuel et KIES Stephen, « Social Media Impact on Attention Span », *Journal of Management & Engineering Integration*, vol. 11, 2018, p. 20-27 ; PAUL Jomon Aliyas, BAKER Hope M. et COCHRAN Justin Daniel, « Effect of online social networking on student academic performance », *Computers in Human Behavior*, vol. 28, 2012, p. 2117-2127 ; en marketing v. KAUR Simperpreet, « Social media marketing », *Asian Journal of Multidimensional Research*, vol. 5, 2016, p. 6-12 ; MAURER Christian et WIEGMANN Rona, « Effectiveness of Advertising on

être directement atteints par le contenu d'une application, ses dysfonctionnements ou les décisions de son gestionnaire.

La métrique du nombre d'utilisateurs actifs/mois (MAU, *Monthly Active Users*) nous intéresse d'autant plus qu'elle trouve progressivement sa place en droit, afin d'échelonner les obligations légales des fournisseurs de service en ligne. Ainsi, du côté européen, le *Digital Services Act* oblige spécifiquement les plateformes qui totalisent plus de 45 millions d'utilisateurs actifs dans l'UE à : fournir un rapport d'évaluation des risques systémiques posés par l'utilisation de sa plateforme au sein de l'UE ainsi qu'un rapport relatant les mesures prises par la plateforme pour atténuer ces risques ; payer un audit extérieur (indépendant) chaque année pour vérifier leur respect du *Digital Services Act* et de leurs engagements au titre des codes de conduite ; désigner un délégué, au sein du personnel ou une personne extérieure, chargé de vérifier régulièrement la mise en conformité de la plateforme avec le *Digital Services Act* ; informer les utilisateurs, dans leurs CGU, des paramètres utilisés pour leurs systèmes de recommandation, et offrir aux utilisateurs la possibilité de désactiver les systèmes de recommandation qui reposent sur du profilage ; ou encore mettre à disposition des utilisateurs une base de données qui indique, jusqu'à un an après le dernier affichage de la publicité, le contenu de cette publicité, la personne pour le compte de laquelle elle est affichée, la période durant laquelle la publicité a été affichée, le caractère ciblé ou générique de la publicité et les critères de ciblage le cas échéant, ainsi que le nombre d'utilisateurs atteints par la publicité¹⁰²³.

Toujours dans l'UE, le *Digital Markets Act* en préparation propose d'imposer certaines obligations spécifiques aux « contrôleurs d'accès », i.e. aux « fournisseurs de services de plateforme essentiels [*services d'intermédiation en ligne, moteurs de recherche, réseaux sociaux, plateformes de partage de vidéos, services de communications interpersonnelles non fondées sur la numérotation, système d'exploitation, service d'hébergement cloud et services de publicités*] » qui ont « un poids important sur le marché intérieur », représentent « un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux » ou encore « jouissent d'une position solide et durable dans [*leurs*] activités ou jouiront, selon toute probabilité, d'une telle position dans un avenir proche »¹⁰²⁴. Un fournisseur de services de plateforme essentiels est présumé être un contrôleur d'accès s'il connecte plus de 10 000 entreprises par an et plus de 45 millions d'utilisateurs actifs par mois situés dans l'UE, ou si son chiffre d'affaires annuel dans l'Espace économique européen est supérieur à 6,5 milliards d'euros, ou encore si la valeur marchande ou la capitalisation boursière de l'entreprise atteinte au moins 65 milliards d'euros¹⁰²⁵. Les contrôleurs d'accès sont à leur tour soumis à certaines obligations et interdictions spécifiques telles que : donner aux entreprises utilisatrices la capacité de promouvoir leurs offres et de conclure des contrats avec les utilisateurs finaux en utilisant ou non un service du contrôleur d'accès ; permettre aux entreprises utilisatrices d'accéder aux données qu'elles génèrent en utilisant la plateforme du contrôleur d'accès ; ne pas privilégier les produits et services proposés par le contrôleur d'accès par rapport aux

Social Network Sites », *Conference: Information and Communication Technologies in Tourism*, Conférence internationale d'Innsbruck des 26 et 28 janv. 2011

¹⁰²³ Règlement (UE) 2022/2065 du 19 oct. 2022 relatif à un marché unique des services numériques, Section 5

¹⁰²⁴ Proposition de Règlement du Parlement européen et du Conseil du 15 décembre 2020 relatif aux marchés contestables et équitables dans le secteur numérique, COM(2020) 842 final, art. 2 et 3

¹⁰²⁵ *Ibid.*, art. 3, 2.

produits et services proposés par les entreprises utilisant sa plateforme ; ne pas conditionner l'accès, l'inscription ou l'enregistrement sur ses serveurs à l'enregistrement des entreprises utilisatrices ou des utilisateurs finaux sur un autre service du contrôleur d'accès ; ne pas empêcher les utilisateurs de désinstaller un logiciel préinstallé etc.¹⁰²⁶ On a vu également que, en Russie, la loi sur l'autorégulation des réseaux sociaux de 2021 impose des obligations spécifiques aux « grands réseaux sociaux », qui rassemblent plus de 500 000 utilisateurs par jour sur le sol russe¹⁰²⁷. On propose le barème suivant pour catégoriser les applications selon le nombre d'utilisateurs actifs qu'elles connectaient chaque mois au dernier semestre 2022 :

Degré d'utilisation des applications en ligne	Nombre total d'utilisateurs actifs/mois (MAU) d'une application	Exemples d'applications (dans l'ordre de la plus utilisée à la moins utilisée)
Applications très utilisées (ou « centrales ») mondialement	Plus de 100 millions	Google Search, YouTube, Facebook, WhatsApp, Pornhub, Wikipédia WeChat, Bing, Taobao, Baidu Search, Reddit, Bilibili, Spotify, MX Taka Tak, Yandex, Dailymotion, Netflix, Fortnite, Discord, Viber, Zoom, UOL, BBC, Zhihu...
Applications couramment utilisées (ou « assez centrales ») mondialement	99.99 millions – 50 millions	Espn, Wattpad, GitHub, Evernote, Shein, Reverso, Baidu Translate (Fanyi Baidu), UberEats, Ele.me, VK, Tinder, Reuters, 360 Mobile Assistant, Ctrip, Ikea, Genshin Impact, Ozon.ru, Ok.ru, Flickr, Vinted, KakaoTalk, ResearchGate, DeepL, Giphy, Tenor...
Applications moyennement utilisées (ou « moyennement centrales ») mondialement	49.99 millions – 10 millions	UrbanDictionary, Mail.ru, Force.com, Udemy, W3Schools, MeetMe, Nextdoor, Counter Strike: Go, Baidu Tieba, Huya, Jeuxvideo.com, Europa.eu, Call of Duty:Modern Warfare, Valorant, CrunchyRoll, YY Live, CSDN, GTA V, Salesforce, Dota 2, Douban...
Applications peu utilisées (ou « peu centrales ») mondialement	9.99 millions – 5 millions	Analvids.com, Momoshop.com.tw, Pcpartipicker.com, Zapier.com, Futbin.com, Pnc.com, Pixlr, Paramountplus.com, Gaymaletube.com, Emag.ro, PandaReader, Chushou TV, Theqoo.net, Loco, Panda TV, Libgen.is...
Applications très peu utilisées (ou « non centrales ») mondialement	Moins de 5 millions	

En croisant plusieurs bases de données¹⁰²⁸, on a passé au crible le MAU de plus de 4 000 applications en ligne. Cette analyse nous a conduit à identifier 265 applications centrales

¹⁰²⁶ *Ibid.*, art. 5 et 6

¹⁰²⁷ V. *supra*

¹⁰²⁸ On a croisé principalement les données suivantes : l'étude de Kepios, WeAre Social et Hootsuite d'octobre 2022 (entreprises spécialisées dans l'analyse des tendances en ligne auprès des investisseurs, v. « The global state of digital in october 2022 », sur *WeAreSocial.com*, 20 octobre 2022) ; la base de données de Semrush (entreprise spécialisée dans l'étude du trafic en ligne) ; les 2 500 sites web les plus populaires d'après le classement proposé par Myip.ms (entreprise spécialisée dans l'analyse des noms de domaines et adresses IP) ; les tops 500 des applications les plus utilisées en Chine entre 2017 et juillet 2019 par IResearchChina (fournisseur de mesure d'audience en ligne des consommateurs en Chine) ; Statista (fournisseur de statistiques issues d'instituts, de données économiques et d'études de marché et d'opinion) ; Appinchina (entreprise spécialisée dans l'étude de marché chinois des applications) ; classement Alexa 2021 (ex-classement par Amazon des applications les plus utilisées selon un ratio nombre d'utilisateurs actifs par mois/nombre de pages visitées par utilisateur d'une application) ; SimilarWeb (fournisseur de données d'audience des sites web, destinées surtout aux entreprises sur le marché numérique) ; dfcfw.com (entreprise spécialisée dans l'étude du marché numérique chinois et dans le conseil aux investisseurs sur ce marché) ; hypestat.com (agrégateur et

mondialement, *i.e.* qui connectent plus de 100 millions d'utilisateurs actifs par mois. On propose en Annexe un classement de ces 265 applications, de la plus utilisée à la moins utilisée. Le classement recense le MAU de chacune de ces applications sur le dernier semestre 2022, ainsi que le type d'application (moteur de recherche, navigateur web, réseau social...) et son propriétaire. Quoique probablement non exhaustive, cette liste se veut la plus complète possible.

Les chiffres répertoriés ne doivent pas être tenus pour absolument exacts en raison : de l'absence de définition universelle des « utilisateurs actifs » (l'utilisateur actif peut être regardé comme celui qui visite régulièrement l'application, ou celui dont la visite est supérieure à 2 minutes, ou encore à 5 minutes...) ; de l'absence d'une autorité qui aurait accès aux statistiques exactes de trafic, de comptes utilisateurs, du taux de duplication (nombre moyen de terminaux utilisés par chaque internaute pour accéder à l'application) ou encore du taux d'adoption des applications en ligne à échelle mondiale ; de fortes discordances entre les chiffres des entreprises d'analyse de trafic web (Semrush, SimilarWeb, Statcounter...), les chiffres des organismes d'analyse des usages en ligne (Kepios et Hootsuite à échelle internationale, iResearch Consulting Group et QuestMobile en Chine, Médiamétrie en France, Mediascope en Russie...), les chiffres parfois avancés par les opérateurs de transmission de données (Yota, Orange...), les chiffres annoncés par les propriétaires des applications, ceux obtenus par les enquêtes d'opinion (Centre Levada, Diplomeo...) et ceux soumis par les organisations d'évaluations statistiques (Statista...). Pour toutes ces raisons, le classement proposé en Annexe doit être vu comme un indicateur approximatif des rapports de force entre les applications sur la base de leur audience mensuelle.

Dans le top 10 des applications les plus utilisées dans le monde, on recense Google Search (3,7-3,8 milliards d'utilisateurs actifs/mois sur le dernier semestre 2022), le navigateur Chrome (MAU de 3,3-3,4 milliards sur la même période), Facebook (MAU de 2,7-2,9 mds), YouTube (MAU de 2,55-2,65 mds), WhatsApp (MAU de 2,1-2,3 mds), Pornhub (MAU de 1,9 mds), Gmail (MAU de 1,85-1,95 mds), Play Store (1,8-1,9 mds), XVideos (MAU de 1,8 mds) et Wikipédia (MAU de 1,7 mds).

On compte vingt applications en ligne qui connectent plus d'un milliard d'utilisateurs actifs par mois (Instagram, App Store, Google Maps, iCloud, WeChat, iMessage, TikTok/Douyin, et probablement Google Translate, Safari et Google Drive en plus des dix précédemment citées). En étudiant l'évolution du MAU de ces diverses applications, on a observé qu'il est exceptionnel pour une application de gagner en une seule année plus de 150 millions de nouveaux utilisateurs actifs/mois. En moyenne, sur une année entière, les applications très utilisées mondialement gagnent ou perdent entre 20 et 80 millions d'utilisateurs actifs/mois. On constate toutefois trois exceptions au moins dans lesquelles une application peut jouir d'un bond spectaculaire, en accroissant son MAU de plus de 150 millions sur une année.

B) *Les bonds exceptionnels des applications fédératrices et novatrices*

Première exception : le MAU d'une application peut bénéficier d'un bond supérieur à 150 millions sur une seule année **lorsque les fonctions de cette application fédèrent des usages dispersés mais déjà largement adoptés par les utilisateurs, à la condition toutefois que cette application popularise au moins une technique ou un usage peut adopté jusqu'à présent**. De cette façon, une application peut récupérer tous les utilisateurs qui adoptaient déjà

comparateur de diverses statistiques de trafic, provenant notamment de Semrush et du classement Alexa 2021) ; finance.sina.com (application chinoise de Sina Corporation traitant de l'actualité économique et financière) ; et divers articles de la presse américaine, indienne, chinoise, japonaise et coréenne

cet usage, tout en se démarquant de la concurrence par la technique ou l'usage nouveau qu'elle popularise. Cette exception est celle grâce à laquelle sont nés la plupart des géants d'internet.

Il en va ainsi du réseau social Facebook. Pour comprendre la rapidité de son succès, on remonte au site web Sixdegrees.com. Né en 1997, Sixdegrees.com était un réseau social assez similaire à Facebook, permettant aux utilisateurs de créer leur profil, d'y publier du contenu, d'inviter leurs amis, familles et collègues parmi leurs contacts, de leur envoyer des messages... Faute d'une bonne vitesse de connexion internet à l'époque, d'un nombre suffisant d'utilisateurs d'internet dans le monde (7% de la population mondiale est connectée à internet en 2000, soit 430 millions de personnes¹⁰²⁹), et dans un contexte où les usages en ligne n'étaient pas encore habitués aux réseaux sociaux, SixDegrees a échoué à connecter un très grand nombre d'utilisateurs actifs (3.5 millions à son apogée¹⁰³⁰). Le service dut fermer en 2001. Entre la fin des années 1990 et le début des années 2000, fleurit une nuée de réseaux sociaux. Vers la fin des années 2000, des centaines de millions d'utilisateurs s'étaient déjà habitués à communiquer par messagerie instantanée (avec Windows Live Messenger né en 1999 et Skype né en 2003), à partager leurs goûts et centres d'intérêt (avec MySpace né en 2003), à partager des textes, images et photos mettant en scène leur quotidien (avec Skyrock né en 2002, Photobucket né en 2003 et Flickr né en 2004), à partager des vidéos (avec YouTube et Dailymotion nés en 2005), à rechercher leurs amis en ligne (avec Copains d'avant né en 2001 et Viadeo né en 2003) et commençaient à s'habituer à lire des informations sur un fil d'actualité (avec Twitter né en 2006). Facebook est né en 2004, mais s'est ouvert hors des campus américains en 2006. Il fédérait à lui seul la plupart des fonctions proposées par ces divers réseaux sociaux très utilisés (messagerie instantanée, partage de vidéos, images et photos, mise en scène de soi, recherche d'amis en ligne...), à un moment où les utilisateurs s'étaient habitués à ces fonctions. Cette différence de contexte entre Facebook et SixDegrees explique probablement l'échec de ce dernier, né à un moment où les utilisateurs ne s'étaient pas encore adaptés aux fonctions des réseaux sociaux¹⁰³¹. En plus de fédérer ces usages et techniques déjà ancrés mais jusqu'alors dispersés sur plusieurs réseaux sociaux, Facebook a popularisé une technique nouvelle – celle du fil d'actualité. Twitter et surtout Facebook ont fait du fil d'actualités un marqueur des réseaux sociaux de partage des contenus dans la décennie 2010 (adopté depuis par Weibo, Instagram, Reddit, Imgur...). À la fois fédérateur d'habitudes et promoteur d'une technique nouvelle et populaire, Facebook a vu en 2010 son MAU profiter de l'un des premiers bonds de l'histoire supérieurs à 150 millions d'utilisateurs actifs/mois¹⁰³².

Le même scénario s'est produit en Chine au début des années 2010 avec WeChat. Sortie le 21 janvier 2011, l'application WeChat n'était qu'une messagerie instantanée textuelle et d'échanges de photos. Les internautes chinois s'étaient déjà largement habitués à ces usages

¹⁰²⁹ « Utilisateurs d'Internet (% de la population) », sur *Donnees.banquemondiale.org*, mis à jour en 2021. Les données mises sous forme de graphique dans ce document sont issues de la base de données de l'Union internationale des télécommunications (UIT) sur le développement des télécommunications / TIC dans le monde.

¹⁰³⁰ « 7 social media sites that failed to become "Facebook" », sur *The Economic Times* [en ligne], 2017

¹⁰³¹ QUINTON François, « Facebook, les raisons du succès. Entretien avec Nikoas Smyrniaos » [en ligne], *INA-La revue des médias*, février 2014

¹⁰³² Facebook a ainsi gagné 250 millions d'utilisateurs actifs/mois entre juillet 2009 (MAU de 250 millions) et juillet 2010 (MAU de 500 millions), puis plus de 200 millions d'utilisateurs actifs/mois entre juillet 2011 et juin 2012 (MAU de 955 millions), v. The Associated Press, « Number of active users at Facebook over the years » [en ligne], sur *Yahoo! Finance*, oct. 2012.

avec QQ né en 1999 (équivalent de Windows Live Messenger), Baidu Tieba né en 2003 (un réseau social de partage de contenus mais dont le MAU a chuté depuis la deuxième moitié des années 2010), Renren né en 2005 (équivalent de Facebook mais dont le MAU a chuté depuis la fin des années 2010)... Trois jours avant WeChat sortait l'application chinoise TalkBox, l'un des premiers réseaux sociaux de messagerie instantanée vocal push-to-talk (l'appui d'un bouton fait passer du mode récepteur au mode émetteur). Le mois suivant, l'application concurrente MiTalk de Xiaomi reprend à son compte la fonction de messagerie vocale push-to-talk innovée par TalkBox, puis, en mai 2011, WeChat intègre une fonction de messagerie instantanée vocale. C'est à ce moment que le MAU de WeChat décolle, augmentant la croissance quotidienne de ses nouveaux utilisateurs actifs de moins de 20 000 à plus de 50 000¹⁰³³. Quelques mois plus tard, le développeur et propriétaire de WeChat, Tencent, popularise un nouvel usage : la fonction « People Nearby » (plus tard reprise par MiTalk avec sa fonction LBS puis par TalkBox), qui permet aux membres de WeChat de découvrir des personnes géographiquement proches avec qui discuter sur la messagerie instantanée. Après l'apparition de cette fonction, la croissance quotidienne des nouveaux utilisateurs actifs de WeChat franchit le seuil des 100 000¹⁰³⁴. WeChat gagne 100 millions d'utilisateurs actifs/mois entre 2011 et 2012, et son MAU bondit pour la première fois de plus de 150 millions entre 2013 et 2014 (passant de 198 millions à 432 millions)¹⁰³⁵. Comme Facebook a fédéré divers usages et fonctions dont une nouvelle fonction qu'il a popularisée (le fil d'actualité), WeChat a fédéré divers usages et fonctions largement adoptés (messagerie instantanée textuelle et de partage d'images) et a popularisé plusieurs fonctions peu adoptées jusqu'alors (messagerie instantanée vocale et géosociale).

On pense que les mêmes raisons (fédération des messageries instantanées textuelles et de partage d'images, popularisation de la nouvelle fonction de messagerie instantanée vocale) expliquent aussi le premier bond exceptionnel de WhatsApp. WhatsApp est diffusée publiquement en 2009, comme une application de messagerie instantanée textuelle et de partage d'images. Or, après avoir intégré la fonctionnalité de messagerie instantanée vocale en 2013, WhatsApp enregistre au premier trimestre 2014 son premier bond supérieur à 150 millions d'utilisateurs actifs (avant le rachat de WhatsApp par Meta la même année)¹⁰³⁶. Tant pour WeChat que pour WhatsApp, leur MAU ne commence à bondir qu'après avoir intégré des fonctions peu adoptées jusqu'à présent (messagerie instantanée vocale et géosociale), sachant que ces deux applications fédéraient déjà des usages largement adoptés (messageries instantanées textuelle et de partage d'images).

¹⁰³³ SHEN Xinmei, « Popular TV show reveals how WeChat crushed a rival messaging app » [en ligne], sur *South China Morning Post*, 12 nov. 2018

¹⁰³⁴ WU Xiaobo, *The Story of Tencent: Evolution of Chinese Internet Companies from 1998 to 2016. The Evolution of the Chinese Internet Company*, Zhejiang University Press, 2017

¹⁰³⁵ MILLWARD Steven, « WeChat still unstoppable, grows to 697m active users » [en ligne], *Tech in Asia*, 17 mars 2016. Les chiffres ici rapportés sont ceux communiqués par Tencent. Ils sont corroborés par l'analyse d'iResearch : « Rapport d'iResearch 2015 sur les habitudes comportementales des utilisateurs de WeChat dans le cadre de l'utilisation de leurs comptes » (微信用户使用公众号行为习惯研究报告 2015 【艾瑞咨询】), sur *Developer.alyun.com* [communauté des développeurs d'Alibaba partageant les captures d'écran de l'étude], 5 juil. 2015

¹⁰³⁶ Le MAU de WhatsApp passe ainsi de 103 millions (2012) à 213 millions (2013), puis à 409 millions (2014) : CECI L., « Number of monthly active WhatsApp users worldwide from April 2013 to March 2020 », *Statista*, 27 juil. 2022. Ces chiffres sont rapportés par Meta, propriétaire de WhatsApp. Ils nous semblent crédibles, d'autant que le MAU de WhatsApp récemment avancé par Meta pour le dernier semestre 2022 (entre 2 et 2,4 milliards d'utilisateurs) est corroboré par plusieurs enquêtes d'opinion : CECI L., « WhatsApp monthly usage in selected markets worldwide as of 3rd quarter 2022 », *Statista*, 16 mai 2023

C'est aussi de cette exception dont a bénéficié Gmail. Gmail est né en 2004, à un moment où plus de 330 millions d'internautes avaient déjà largement adopté l'usage des boîtes de messagerie en ligne (MSN Hotmail, NetEase Mail, AOL Mail, Yahoo! Mail, QQ Mail, Docomo Mail, NAVER Mail, Mail.ru...) ¹⁰³⁷. En octobre 2007, Gmail permet à ses utilisateurs de stocker leurs emails sur des serveurs de la société Alphabet (propriétaire de Gmail) plutôt que sur le terminal de l'utilisateur ¹⁰³⁸. Le stockage des mails n'est donc plus limité par l'espace mémoire qu'offre un terminal, mais par celui qu'offrent des serveurs dotés d'une très grande capacité mémoire (serveurs *cloud*). Dès lors, Gmail est devenue la première boîte de messagerie à offrir à ses utilisateurs un espace mémoire (1Go contre quelques dizaines de Mo chez les concurrents) tel que les utilisateurs pouvaient constamment envoyer et recevoir des emails sans être obligés de supprimer régulièrement leurs mails et de vider la corbeille pour libérer l'espace de stockage des emails. Gmail fut aussi la première boîte de messagerie à filtrer activement les spams, à supprimer les bannières publicitaires, et à actualiser automatiquement des emails. Toutes ces fonctions ont ensuite été progressivement reprises par les concurrents, illustrant à quel point Gmail a popularisé ces techniques sur le marché des boîtes de messagerie. À la fois fédérateur d'usages déjà largement adoptés (l'utilisation d'une boîte de messagerie) et promoteur de nouveaux usages et fonctions qui l'ont démarqué de la concurrence (disparition des bannières publicitaires, des obligations de suppression et d'actualisation des mails, filtrage des spams...), Gmail a vu son MAU bondir exceptionnellement pour la première fois entre 2011 et 2012, passant de 272 à 443 millions ¹⁰³⁹.

On prend pour dernier exemple l'ascension fulgurante de TikTok, un réseau social exclusivement consacré au partage de courtes vidéos. Avant TikTok, d'autres réseaux sociaux se consacraient uniquement au partage de courtes vidéos : Vine né en janvier 2013, sur le marché occidental ; Meipai (美拍) né en mai 2014 et Miaopai (秒拍) en juillet 2014, sur le marché chinois. Le succès de Vine, de Miaopai et de Meipai fut immédiat, sans toutefois que leur MAU bondisse de plus de plus de 150 millions sur une seule année. Applications gratuites les plus téléchargées sur l'App Store dès leur lancement, Vine atteint 200 millions d'utilisateurs actifs/mois en décembre 2015, Meipai plus de 150 millions en 2017 et Miaopai plus de 40 millions la même année ¹⁰⁴⁰.

Vine, Miaopai et Meipai sont nés à un moment (2013-2014) où la fonction de partage de courtes vidéos n'était pas encore largement adoptée, donc à un moment où cette fonction ne pouvait pas fédérer rapidement un grand nombre d'usages existants. Vine n'offrait quasiment pas d'outil d'édition de vidéos, de façon que la création de courtes vidéos se résumait à filmer des situations sans le moindre ajout. Les créateurs pouvaient alors difficilement élaborer des vidéos attractives, et les « perles » de Vine étaient rares et fastidieuses à trouver. Les utilisateurs

¹⁰³⁷ « Most Popular Email Providers in History », sur *Statisticsanddata.org*, 2021. Statistics and Data est un projet de recherche, d'analyse et de visualisation de données.

¹⁰³⁸ JONES K.C., « Gmail Now Has IMAP Support », sur *InformationWeek.com*, oct. 2007

¹⁰³⁹ « Most Popular Email Providers in History », sur *Statisticsanddata.org*, préc.

¹⁰⁴⁰ D'après les chiffres annoncés par les propriétaires des applications : « Rapport de recherche sur les actions financières – Recherche sur l'industrie – Industrie des médias et d'internet. Recherche approfondie de la série Consumer Upgrade (4) : courte vidéo » (证券研究报告-行业研究•传媒与互联网行业. 消费升级系列深度研究 (4) : 短视频) [en ligne], *Soochow Securities*, 17 sept. 2017, p. 33 ; « Miaopai : 7,55 millions d'activités quotidiennes, 2,65 milliards de lectures quotidiennes, le fonctionnement et l'art de l'exploitation des données des courtes vidéos » (秒拍: 755 万日活, 26.5 亿次日播放, 短视频数据运营的道与术), sur *sq.sf.163.com*, 18 mai 2018

ont peu à peu quitté Vine pour partager leurs courtes vidéos sur des réseaux sociaux qui leur offraient des outils d'édition tels que l'ajout de musiques de fond sur les vidéos créées ([Musical.ly](#) né en avril 2014) ou sur des réseaux sociaux dont les fonctions fédéraient des usages déjà largement adoptés (Instagram dont la fonction de partage de contenus fédère des usages déjà largement adoptés et qui intègre un outil de partage et d'édition de courtes vidéos en juin 2013, YouTube dont la fonction de partage de vidéos est déjà largement adoptée et qui héberge de plus en plus de compilations de courtes vidéos, Snapchat dont la fonction de messagerie instantanée est déjà largement adoptée et sur lequel les utilisateurs partagent de plus en plus de courtes vidéos...). Face à l'éclosion de sa base d'utilisateurs, Twitter Inc., propriétaire de Vine, annonce la fermeture du service en octobre 2016. Sur le marché chinois, Miaopai suit le même chemin. Bien qu'étant originellement un clone de Vine, Miaopai intègre vers 2014-2015 une palette complète d'outils d'édition des vidéos (musiques, filtres et effets visuels, jeux de lumière, thèmes, caractères...), de façon à stimuler l'inventivité des créateurs de vidéos et l'attentivité des visiteurs. Cependant, adossé à Weibo (réseau social de microblog), l'usage de Miaopai se réduisait au microblog et limitait le nombre de ses utilisateurs à ceux de Weibo. Les utilisateurs de Miaopai se sont alors éparpillés sur des réseaux sociaux dont les fonctions fédéraient des usages déjà largement adoptés (messagerie instantanée comme Kuaishou, partage de contenus comme Toutiao, Xiaohongshu...), ou sur des applications concurrentes qui offraient des outils d'édition de courtes vidéos (Toutiao Video, Meipei, Xiaokaxiu...). Le MAU de Miaopai, évalué à 150 millions mi-2017, chute à 98 millions fin 2017 puis à 42 millions en juin 2018¹⁰⁴¹.

TikTok surgit en septembre 2016, dans **un contexte où la fonction de partage de courtes vidéos est déjà** largement adoptée (popularisée par Vine, Miaopai et Meipei), **donc fédératrice en elle-même, mais dispersée sur une foule de réseaux sociaux** (Instagram, YouTube, Snapchat, Twitter, [Musical.ly](#), Pinterest, Kuaishou, Toutiao, Toutiao Video, Xiaohongshu, Xiaokaxiu,...). Ce contexte offrait à TikTok la possibilité de fédérer rapidement un grand nombre d'utilisateurs dès son arrivée sur le marché. Il y parvient en activant trois leviers. Lancé sur le marché chinois sous le nom de [A.me](#), devenu Douyin depuis décembre 2016, il joue d'abord sur l'effet d'apprentissage acquis par les utilisateurs. Habités depuis 2015-2016 à manier les outils d'édition de courtes vidéos, les internautes chinois ont appris à créer des contenus de qualité et leurs vidéos sont donc de plus en plus attractives. Douyin stimule à la fois la créativité des utilisateurs en leur fournissant une palette très complète d'outils d'édition vidéo (notamment des effets visuels sophistiqués et faciles d'utilisation) et l'attractivité des vidéos en les faisant défiler les unes après les autres sur la page d'accueil de l'utilisateur sans laisser à ce dernier le choix entre plusieurs vidéos. Pariant sur l'inventivité suscitée par ses outils et sur la qualité des contenus que son algorithme sélectionne pour l'utilisateur, Douyin priorise la créativité et l'attractivité du contenu à un moment où les utilisateurs commençaient à maîtriser la création de courtes vidéos et à rechercher ce format sur internet. Inversement, Meipei priorise l'interactivité suscitée par le contenu en s'axant sur le partage en direct de courtes vidéos, au détriment de la créativité et de l'attractivité du contenu (outils d'édition moins diversifiés et sophistiqués, plus difficiles à manier en direct...) ¹⁰⁴².

¹⁰⁴¹ JUAN Chen et JING Liu, « Meitu Shares Fall to All-Time Low on Disappointing First Half Results », sur [Ycaiglobal.com](#), 22 août 2018

¹⁰⁴² Fondé en 2014 sur l'édition de courtes vidéos, Meipei a pris un tournant en janvier 2016 en intégrant la fonction de partage en direct de courtes vidéos, dans le but de stimuler les interactions avec les influenceurs qui peuvent communiquer en direct avec leur public via de courtes vidéos (« Diffusion en direct sur l'application Meipei : la beauté instantanée » (美拍 App 直播功能上线 即时美

Le deuxième levier mobilisé par la société ByteDance Limited a consisté à faire de son application Douyin un réseau social autonome et ouvert. Contrairement à Miaopai et à Toutiao Video, qui sont des segments de Weibo et de Toutiao, Douyin est un réseau social qui ne dépend d'aucun autre et qui s'adresse génériquement à tous les utilisateurs (plutôt qu'à une communauté de microblog ou de partage de contenus). La progression du MAU de Douyin n'a donc pas été plafonnée par le MAU d'un autre réseau social. Créatif, attractif, autonome et ouvert à tous, Douyin devient rapidement le réseau social de courtes vidéos le plus utilisé en Chine. Son MAU dépasse celui de Miaopai en juin 2017 (5 millions pour Miaopai contre 7 millions pour Douyin), puis dépasse celui de Meipai en août 2017 (32 millions pour Meipei contre 38 millions pour Douyin), franchit le seuil des 100 millions en janvier 2018, et dépasse le MAU de Kuaishou en juillet 2018 (259 millions pour Kuaishou contre 262 millions pour Douyin) ¹⁰⁴³. Le MAU Douyin fait son premier bond exceptionnel entre juin 2017 et juin 2018, passant de 5 millions à 232 millions.

Persistant sa stratégie d'ouverture, ByteDance lance en 2017 une version de Douyin sur le marché international, appelée TikTok. ByteDance exploite ici son troisième levier : le rachat de la concurrence. En novembre 2017, il acquiert son principal concurrent sur le marché international de l'édition de courtes vidéos, [Musical.ly](https://www.musical.ly), faisant de TikTok en janvier 2018 le seul réseau social très utilisé mondialement exclusivement dédié à l'édition de courtes vidéos. On sait que, en 2018, les fonctions de partage et d'édition de courtes vidéos sont fédératrices à elles seules d'usages largement adoptés. Dans ce contexte, TikTok / Douyin est devenu le réseau social mondialement fédérateur de ces usages, et son MAU a fusé en gagnant près de 300 millions supplémentaires chaque année entre 2018 et 2022 ¹⁰⁴⁴. Le succès de TikTok a popularisé deux fonctions nouvelles : la créativité stimulée par la richesse des outils d'édition vidéo ; et l'attractivité stimulée par une page d'accueil unique proposant à l'utilisateur des vidéos créatives sans qu'il ait à les chercher lui-même ¹⁰⁴⁵. Cette popularisation s'observe par la quantité de réseaux sociaux très utilisés mondialement qui ont inséré des fonctions d'édition et de partage de courtes vidéos (Imgur en juin 2018) voire qui ont, en plus, reproduit la page unique d'accueil faisant défiler les courtes vidéos (YouTube Shorts né en juillet 2021, onglet de courtes vidéos de Reddit depuis août 2021...), sans compter les nombreux réseaux sociaux nés après TikTok et

顏超神奇), *China Times*, 26 janv. 2016 ; « Meipai » (美拍), *Baike Baidu* [encyclopédie chinoise en ligne] ; « [Meipai] Rapport d'expérience produit » ([美拍]-产品体验报告), *Zhihu* [réseau social chinois de questions-réponses], 19 sept. 2017). Un réseau social fondé sur l'interactivité a pour avantage de rendre son MAU plus solide car il approfondit les relations entre les membres de sa communauté. Cela explique probablement que le MAU de Meipei se soit stabilisé à 20-25 millions quand celui de Miaopai s'est effondré à moins de 5 millions. Cependant, Meipei ne s'est pas appuyé sur l'effet d'apprentissage pour rendre son contenu créatif et attractif, ce qui l'a probablement empêché d'élargir sa communauté.

¹⁰⁴³ Sur l'évolution du MAU de TikTok, les rapports mensuels d'iResearch China, « Top 500 Apps in China by UVs » des mois de juin 2017, août 2017, janvier 2018 et juillet 2018 [en ligne]

¹⁰⁴⁴ Le MAU de TikTok / Douyin est ainsi passé de 55 millions (janvier 2018) à 178 millions (mi 2018), puis à 419 millions (mi 2019), à 689 millions (mi 2020), à 930 millions (mi 2021) et à un peu plus de 1,1 milliard (mi 2022). Chiffres obtenus par croisement des données d'iResearch avec CECI L., « Number of monthly active users (MAU) of TikTok worldwide from January 2018 to September 2021 », *Statista*, 29 juil. 2022 et CECI L., « Number of TikTok users worldwide from 2020 to 2025 », *Statista*, 5 sept. 2022

¹⁰⁴⁵ *A contrario*, la découverte de vidéos courtes par les utilisateurs se faisait par catégories (onglets) de contenus sur Miaopai, et principalement par recherche de profils de créateurs sur Meipei (plus proche d'Instagram) : v. notam. All Tech Asia, « Miaopai: from a Vine clone to a tech unicorn in 2 years », sur *Medium.com*, fév. 2016

devenus très utilisés mondialement qui se sont exclusivement consacrés au partage de courtes vidéos en reprenant la combinaison des outils d'édition et de la page d'accueil unique (Huoshan de ByteDance né en décembre 2016, Likee né en juillet 2017, Moj et MX Taka Tak nés en en juillet 2020, Josh né en septembre 2020...).

C) Les bonds exceptionnels des applications du fait de leur insertion ou de circonstances extraordinaires

Deuxième exception : le MAU d'une application peut bénéficier d'un bond supérieur à 150 millions **lorsque les fonctions de cette application s'insèrent parfaitement avec les fonctions d'un autre programme très utilisé mondialement**. Ce fut la tentative de Miaopai, dont le partenariat avec Weibo offre un accès facilité à Miaopai depuis Weibo. Du fait de son insertion avec Weibo, Miaopai a bénéficié dès sa naissance d'une visibilité auprès des 150 millions d'utilisateurs de Weibo en 2014, ce qui a probablement joué un rôle déterminant dans son succès immédiat. On a vu cependant que cette stratégie d'insertion s'est retournée contre Miaopai en l'enfermant sur Weibo, le privant de devenir le réseau social autonome, générique et ouvert qu'est devenu TikTok / Douyin.

Cependant, **la stratégie de l'insertion peut être très efficace lorsque l'application s'articule avec le fonctionnement même d'un programme très utilisé mondialement**. Un premier exemple est celui de l'application iCloud d'Apple, qui synchronise automatiquement des données entre tous les appareils Apple d'un utilisateur (ordinateur Mac, iPhone, tablette iPad, écouteurs AirPods...), permet le suivi des appareils en cas de perte sur icloud.com, le stockage de tous fichiers téléchargés par l'utilisateur (images, photos, vidéos, musiques, texte etc.) ... iCloud est si parfaitement inséré au fonctionnement d'iOS, de macOS et de PadOS (systèmes d'exploitation des iPhone, ordinateurs Mac et iPads) que son MAU a pu suivre la croissance du MAU d'Apple. La société Apple annonçait ainsi en février 2016 que 78% de ses utilisateurs actifs se servaient d'iCloud au moins une fois par mois¹⁰⁴⁶. On en déduit qu'iCloud a probablement gagné 78% des 720-790 millions d'utilisateurs d'Apple à la mi 2016¹⁰⁴⁷, soit 560-615 millions d'utilisateurs un peu plus de quatre ans après son lancement en octobre 2011 (croissance moyenne du MAU d'iCloud de 120 millions supplémentaires chaque année entre 2011-2016). Par ailleurs, le nombre d'utilisateurs actifs d'iPhones a exceptionnellement bondi de plus de 200 millions (passant de 1,1-1,15 milliard à 1,3-1,4 milliard)¹⁰⁴⁸. On estime que le MAU d'iCloud a bondi la même année de 145 à 165 millions d'utilisateurs (passant de 830-885 millions en 2020 à 985 millions-1,05 milliards en 2021)¹⁰⁴⁹.

¹⁰⁴⁶ AppleInsider Staff, « Apple Music passes 11M subscribers as iCloud hits 782M users », sur *Appleinsider.com*, 12 fév. 2016

¹⁰⁴⁷ CYBART Neil, « Apple's Billion Users », *Above Avalon* [en ligne, entreprise spécialisée dans l'analyse d'Apple], 30 mai 2019. Business of Apps dénombrait 710 millions d'utilisateurs actifs d'iPhones la même année : CURRY David, « Apple Statistics », *Business of Apps* [en ligne], mis à jour le 2 mai 2023

¹⁰⁴⁸ *Ibid.*

¹⁰⁴⁹ On a effectué cette estimation de la façon suivante : Apple a gagné plus de 200 millions d'utilisateurs actifs entre 2020 et 2021. L'appareil le plus expédié par Apple en 2021 fut l'iPhone – 1.35 milliards d'iPhones expédiés en 2021, contre 100-150 millions d'écouteurs AirPods, 58 millions d'iPads et 25 millions d'ordinateurs Mac la même année (sur *Statista.com* : LARICCHIA Federica « Smartphone unit shipments worldwide 2007-2021, by vendor », oct. 2022 ; LARICCHIA F., « Global true wireless stereo (TWS) units shipped in Q1 2020, Q2 2020 and Q2 2021 by brand », mai

De même, la stratégie de l'insertion peut être très efficace lorsque l'application s'articule avec les usages faits d'un programme très utilisé mondialement. Prenons l'exemple d'un programme très utilisé mondialement : le système d'exploitation des smartphones Android, dont est propriétaire Alphabet, et qui totalise entre 3,1 et 3,3 milliards d'utilisateurs actifs/mois au dernier semestre 2022¹⁰⁵⁰. Or, avec les magasins d'applications qui se sont popularisés depuis la fin des années 2000, les internautes utilisent fréquemment leur smartphone pour télécharger des applications. Le magasin d'applications d'Alphabet, Play Store, s'articule très bien avec cet usage des smartphones, ce qui lui a permis de suivre la croissance du MAU d'Android. Or, Android a fait de nombreux bonds exceptionnels depuis son lancement en septembre 2008. On relève son premier bond entre 2012 et 2013 où son MAU gagne 200 millions (passant de 500 à 700 millions). Son MAU gagne ensuite 300 millions entre 2013 et 2014 (passant de 700 millions à un milliard), 400 millions entre 2014 et 2015 (passant de 1 milliard à 1,4 milliard), 300 millions entre 2015 et 2016 (passant de 1,4 md à 1,7 md), 300 millions entre 2016 et 2017 (passant de 1,7 md à 2 mds), 300 millions entre 2017 et 2018 (passant de 2 mds à 2,3 mds), 200 millions entre 2018 et 2019 (passant de 2,3 mds à 2,5 mds), 300 millions entre 2019 et 2020 (passant de 2,5 mds à 2,8 mds), et 200 millions entre 2020 et 2021 (passant de 2,8 mds à 3 mds)¹⁰⁵¹.

En 2021, le vice-président de la gestion de produits d'Alphabet révélait que Play Store comptait 2,5 milliards d'utilisateurs/mois – soit 80% à 85% des utilisateurs d'Android¹⁰⁵². À

2022 ; LARICCHIA F., « Apple's global tablet unit shipments from 1st quarter 2012 to 3rd quarter 2022 », nov. 2022 ; LARICCHIA F., « Global unit shipments of Apple Mac computers from 1st quarter 2006 to 3rd quarter 2022 », nov. 2022). Les nouveaux utilisateurs d'Apple en 2021 semblent donc être très majoritairement des utilisateurs d'iPhones, dont le fonctionnement et le graphisme s'insèrent très bien avec iCloud (qui bénéficiait en 2016 d'un taux d'adoption de 75-80% par les utilisateurs d'iPhone). En considérant que le taux d'adoption a légèrement augmenté depuis 2016 (par habitude des utilisateurs au stockage en cloud), on l'a relevé à 80-85%. Autrement dit, on a considéré que le MAU d'iCloud a profité de 80 à 85% du bond de 190 millions effectué par Apple en 2021, soit 150 à 160 millions d'utilisateurs actifs parmi les 190 nouveaux millions de 2021. On a enfin appliqué une marge d'erreur de 5 millions.

¹⁰⁵⁰ Ces chiffres sont ceux annoncés par Alphabet, propriétaire d'Android : CURRY David, « Android Statistics », *Business of Apps*, mis à jour le 27 fév. 2023. Ils nous semblent crédibles. En effet, en 2022, on dénombrait 6,6 milliards de smartphones actifs dans le monde pour 5 milliards d'utilisateurs de smartphones (TAYLOR Petroc, « Number of smartphone mobile network subscriptions worldwide from 2016 to 2022, with forecasts from 2023 to 2028 » ; DEGENHARD J., « Number of smartphone users worldwide from 2013 to 2028 », *Statista*, 1^{er} juin 2023). Or, d'après les analyses de trafic, Android représentait en 2022 environ 71% du marché des systèmes d'exploitation mobiles, soit 71% de 6,6 milliards de smartphones actifs (« Mobile Operating System Market Share Worldwide. Jan – Dec. 2022 », *StatCounter*). D'après ces chiffres, le système d'exploitation Android représente environ de 4,6 milliards de smartphones, et les systèmes d'exploitation d'Apple en représentait environ 1,7 milliards. Les 4,6 milliards de smartphones Android incluent ceux présents en Chine. En effet, le système d'exploitation Android est un logiciel libre, donc réutilisable par n'importe quel fabricant de smartphones (Huawei, Lenovo...) ; mais l'utilisation faite d'Android en Chine continentale n'inclut pas les applications d'Alphabet (Google Maps, YouTube, Google Search...). Sur les 4,6 milliards de smartphones Android, plus d'un milliard d'entre eux sont actifs en Chine sans inclure les applications d'Alphabet. On peut donc estimer à environ 3,1 milliards le nombre de smartphones Android qui proposent l'environnement d'applications Alphabet, ce qui correspond exactement au chiffre annoncé par Alphabet pour 2021 (v. l'étude citée au début de cette note de bas de page).

¹⁰⁵¹ *Ibid.*

¹⁰⁵² Le vice-président annonçait alors que le nombre d'appareils actifs Android venait de franchir le seuil des 3 milliards (v. CRANZ Alex « There are over 3 billion active Android devices »,

l'appui de ces chiffres, en pratiquant la même méthode de calcul que pour iCloud, on estime que le MAU de Play Store se situe entre 2,55 et 2,7 milliards fin 2022 (80 à 85% de 3,1 à 3,2 milliards). Dans cette configuration, on juge probable que le MAU de PlayStore ait fait ses premières bonds exceptionnels vers 2012-2013, en même temps qu'Android. Il est par ailleurs très probable que Gmail et Google Search – qui s'articulent très bien avec les usages faits d'un smartphone (messagerie et recherche Web) – aient eux aussi largement bénéficié de leur insertion avec Android. Ou encore, la principale régie publicitaire d'Alphabet, Google Ads, consiste à déposer des publicités sur Google Search par achat de mots-clés. Google Ads s'insère si bien avec les usages faits de Google Search (2.65 - 2.7 milliards d'utilisateurs actifs/mois de Google Ads au dernier semestre 2022, soit une croissance moyenne du MAU de Google Ads d'environ 115 millions supplémentaires chaque année depuis 2004) qu'il a aussi de toute évidence profité de la croissance du MAU de Google Search (4.5 - 5 milliards d'utilisateurs actifs/mois au dernier semestre 2022, soit une croissance moyenne du MAU de Google Search d'environ 250 millions supplémentaires chaque année depuis 2004).

Troisième exception : le MAU d'une application peut bénéficier d'un bond supérieur à 150 millions **lorsque des circonstances de crise la rendent spécialement intéressante pour les utilisateurs, voire indispensable.** Par exemple, en janvier 2021, la société Meta (alors Facebook) met fin à la séparation qui valait jusqu'à présent entre la messagerie chiffrée WhatsApp et le groupe Facebook : WhatsApp annonce changer ses conditions d'utilisation pour autoriser Meta à croiser toutes les métadonnées des utilisateurs de WhatsApp (numéro de téléphone, nom, adresse IP de l'utilisateur et de ses contacts...) avec celles des utilisateurs de Facebook, Instagram et FB Messenger, et pour autoriser Meta à partager ces données avec ses divers partenaires publicitaires¹⁰⁵³. S'ensuit une crise de réputation pour WhatsApp, sous le feu des critiques des autorités européennes de régulation des données personnelles et des défenseurs du droit au respect de la vie privée¹⁰⁵⁴. Cette crise de réputation profite principalement à une messagerie instantanée chiffrée alternative à WhatsApp : Telegram, qui connectait déjà 400 millions d'utilisateurs en avril 2020¹⁰⁵⁵. Trois jours seulement après le changement de politique de confidentialité de WhatsApp, Telegram gagne 25 millions d'utilisateurs, et le nombre de téléchargements de Telegram atteint son pic historique au mois de janvier 2021 (passant de 32 millions en décembre 2020 à 71 millions en janvier 2021)¹⁰⁵⁶.

Par effet de réseau, cette hausse soudaine du nombre d'utilisateurs a augmenté l'utilité de Telegram pour ses autres utilisateurs, prolongeant ainsi l'augmentation du MAU de Telegram

TheVerge.com, mai 2021), pour 2,5 milliards d'utilisateurs actifs mensuels de Play Store en juillet 2021 (v. « Comment fonctionne Google Play » sur *Play.google.com*).

¹⁰⁵³ « Quatre questions sur la nouvelle politique de partage de données entre Facebook et WhatsApp » [en ligne], *France Info*, 12 janv. 2021

¹⁰⁵⁴ « WhatsApp partagera vos données avec Facebook », *Que choisir* [en ligne], 9 janv. 2021 ; REYNAUD Florian, « WhatsApp modifie sa politique de confidentialité aujourd'hui, voici ce qui changera pour vous », *Le Monde*, 12 mai 2021 ; « Les nouvelles conditions d'utilisation de WhatsApp front l'objet d'une enquête par la Cnil irlandaise » [en ligne], *L'Usine Digitale*, 15 juil. 2021

¹⁰⁵⁵ D'après les chiffres annoncés par le propriétaire de Telegram, Pavel Durov : « Telegram passe les 400 millions d'utilisateurs, les appels vidéo de groupe cette année », *NextInPact*, 27 avr. 2020

¹⁰⁵⁶ « Telegram says 25 million joined in last 72 hours; crosses 500 million users », *The Indian Express* [en ligne], 13 janv. 2021 ; « Number of Telegram app downloads worldwide from January 2019 to February 2023 », *Statista*, 3 mars 2023

sur toute l'année 2021¹⁰⁵⁷. Le MAU de Telegram fait son premier (et unique) bond exceptionnel entre mi 2020 et mi 2021, passant de 400 millions à 550 millions¹⁰⁵⁸. La crise de réputation de WhatsApp ne s'est pas traduite par une réduction de son MAU, mais par un net ralentissement de la croissance de son MAU, passant de 2,06 milliards en janvier 2021 à 2,2 milliards en janvier 2022¹⁰⁵⁹.

Une circonstance de crise peut aussi prendre la forme d'un effondrement soudain d'une application très utilisée mondialement, ou d'une crise sociale, politique, sanitaire... La pandémie de Covid19 survenue en 2020 a par exemple fait émerger une application jusqu'alors peu voire très peu utilisée mondialement : l'application de messagerie instantanée par vidéoconférences Zoom. Contre la pandémie, de nombreux États ferment totalement ou partiellement des écoles et universités, et exigent des entreprises qu'elles privilégient le télétravail. Zoom permet aux élèves d'assister virtuellement au cours que leur professeur diffuse en direct, et aux équipes d'entreprises de s'organiser par vidéoconférences. En temps de distanciation sociale, et soutenu par plusieurs systèmes éducatifs notamment aux États-Unis et dans l'UE, le nombre de participations quotidiennes à des conférences Zoom passe de 10 millions en décembre 2019 à 200 millions en mars 2020 (un mois et demi après le premier confinement italien, un mois après les premiers confinements français, allemand et britannique), puis à 350 millions en décembre 2020¹⁰⁶⁰. Quant au MAU de Zoom, on pense probable qu'il ait pu bondir de 150

¹⁰⁵⁷ Une autre messagerie instantanée chiffrée a bénéficié de la crise de réputation de WhatsApp : Signal. Lors de la polémique de janvier 2021, Elon Musk et Edward Snowden avaient appelé les internautes à quitter WhatsApp pour y préférer Signal, réputé pour la sécurité de sa méthode de chiffrement des données (SMITH Adam, « Leaving WhatsApp will be hard – but it is the right thing to do », *The Independent*, 16 janv. 2021). Comme Telegram, le nombre de téléchargements de Signal a connu son pic historique en janvier 2021, avec 80 millions de téléchargements sur le premier trimestre 2021 - contre seulement 4 millions au dernier trimestre 2020 (CECI L., « Number of Signal app downloads worldwide from 1st quarter 2020 to 2nd quarter 2022 », sur *Statista.com*, nov. 2022). Signal est loin de la base d'utilisateurs de Telegram (12 millions d'utilisateurs actifs pour Signal au dernier trimestre 2020 contre 400 millions pour Telegram), et n'a donc pas pu profiter du même effet de réseau que Telegram (dès lors que Signal connecte un moindre nombre d'utilisateurs actifs, l'utilité sociale de Signal est moindre par rapport à celle de Telegram). Bien que la majorité des internautes ait privilégié le réseau social le plus utile socialement (à savoir Telegram), Signal a tout de même bénéficié d'un effet de réseau notable qui a poussé son MAU de 20 millions en décembre 2020 à 52-58 millions fin 2021 (sur le MAU de 20 millions en décembre 2020, v. SINGH Manish, « Signal's Brian Acton talks about exploding growth, monetization and WhatsApp data-sharing outrage », sur *Techcrunch.com*, janv. 2021 ; sur l'estimation du nombre d'utilisateurs en 2021, on l'effectue à partir du nombre de téléchargements de Signal en 2021, à savoir environ 105 millions de téléchargements pour environ 35 millions de nouveaux utilisateurs actifs, v. l'étude citée dans cette note sur les téléchargements de Signal). Au vu du nombre de téléchargements de Signal en 2022 (à peu près 35 millions), on estime que le MAU de Signal se situe cette année entre 50 et 70 millions.

¹⁰⁵⁸ TALANT Bermet, « How journalists can address misinformation on Telegram », Thomson Reuters Foundation, oct. 2021

¹⁰⁵⁹ CECI L., « Number of unique WhatsApp mobile users worldwide from January 2020 to June 2022 », *Statista*, 15 août 2022

¹⁰⁶⁰ « Zoom says it has 300 million daily meeting participants, not users », *Reuters*, 30 avr. 2020 ; VAILSHERRY Lionel Sujay, « Zoom Video Communications daily meeting participants worldwide from 2019 to 2020 », *Statista*, 11 août 2022 ; « As the world reopens, can Zoom maintain its hold on face-to-face meetings? », *Fortune*, 7 déc. 2021

millions sur une seule année. On situe en effet le MAU de Zoom entre 110 et 160 millions en décembre 2020¹⁰⁶¹, contre probablement 5-8 millions en 2019.

Mise à part Zoom, de nombreuses autres applications ont bénéficié de la pandémie : le MAU de Facebook a enregistré son bond historique le plus important entre 2019 et 2020 en gagnant 280 millions supplémentaires (passant de 2.43 à 2.71 milliards) ; sous la barre des 20 millions entre 2016 et juillet 2019, le MAU de la messagerie instantanée professionnelle Microsoft Teams (concurrente de Zoom sur le marché de la communication en entreprise) bondit subitement entre novembre 2019 et octobre 2020 en passant de 30-35 millions à 200 millions en octobre 2020 alors que le télétravail se généralisait consécutivement à la pandémie, puis atteint 250 millions en 2020, 270 millions en 2021 et 280 millions fin 2022¹⁰⁶² ; de même, le MAU de l'application de paiement

¹⁰⁶¹ Le nombre de participants quotidiens à des conférences Zoom n'est révélateur ni du nombre d'utilisateurs actifs/jour, ni du nombre d'utilisateurs actifs/mois. Une personne qui participe à 5 conférences dans une même journée sera comptée comme 5 participants (WARREN Tom, « Zoom admits it doesn't have 300 million users, corrects misleading claims », sur *TheVerge.com*, avr. 2020). Pour estimer le MAU de Zoom, on s'appuie sur le fait que Zoom confirmait, en décembre 2020, entretenir des partenariats avec 125 000 établissements scolaires et universitaires dans 25 pays différents (« Teaching, Learning & Connecting in 2020: Education in an Extraordinary Year », sur *Blog.zoom.us*, 21 déc. 2020). On doute que ces 125 000 établissements aient été fermés simultanément, et on teste alors deux hypothèses : l'une dans laquelle 90 000 de ces 125 000 établissements scolaires ont été fermés durant un même mois ; et l'autre dans laquelle 60 000 de ces 125 000 établissements scolaires ont été fermés durant un même mois. En nous appuyant sur le nombre d'inscrits dans les établissements scolaires d'enseignement primaire, secondaire et supérieur en 2020 aux États-Unis et dans l'UE, on obtient une moyenne de 88 millions d'élèves et enseignants pour 90 000 établissements scolaires aux États-Unis et dans l'UE. Sur la base des mêmes données, on obtient une moyenne de 64 millions d'élèves et enseignants pour 60 000 établissements scolaires aux États-Unis et dans l'UE. Dans ces deux hypothèses, on a légèrement privilégié le nombre d'étudiants à l'université, plus connectés à Zoom en raison de la fermeture durable et plus généralisée des facultés. Outre le monde éducatif, Zoom est aussi très utilisé dans le monde de l'entreprise. En octobre 2020, Zoom annonçait que 433 700 entreprises utilisaient son application (« Zoom User Statistics: How Many People Use Zoom In 2023 ? » sur *Searchlogistics.com*, janv. 2023). D'après les chiffres donnés par Zoom, c'est 17.5 fois d'entreprises plus qu'en janvier 2018 – 25 800 entreprises utilisaient Zoom –, 8.9 fois plus qu'en janvier 2019 et 6 fois plus qu'en octobre 2019 (*ibid.*). Proportionnellement à cette évolution, et en considérant que le MAU de Zoom se situait entre 5-8 millions pour 10 millions de participations quotidiennes en décembre 2019, on estime que le MAU de Zoom a pu gagner entre 40 et 60 millions d'utilisateurs du côté des employeurs et des employés en 2020. En additionnant ce chiffre avec le nombre d'utilisateurs de Zoom en 2009 (environ 5 millions), et en y ajoutant l'hypothèse des fourchettes hautes (88 millions) et basses (66 millions) du nombre d'élèves et enseignants qui utilisaient Zoom à son pic de décembre 2020, on arrive à une estimation du MAU de Zoom de 110 à 160 millions d'utilisateurs à son pic de décembre 2020, en incluant une marge d'erreur de 5 millions. Cette estimation nous semble par ailleurs cohérente avec le nombre de téléchargements de Zoom sur l'année 2020 – 485 millions (« Zoom User Stats: How Many People Use Zoom in 2022 ? », *Backlinko.com*, 2022) ce qui, proportionnellement au nombre de téléchargements des messageries instantanées WeChat, WhatsApp et Telegram, équivaut à 150-170 millions de nouveaux utilisateurs mensuels (sachant que les élèves et enseignants n'utilisaient Zoom que quand leur établissement était fermé).

¹⁰⁶² REDMOND Tony, « Teams Reaches 280 Million Users as Microsoft Cloud Growth Slows », sur *Office365itpros.com*, 26 janv. 2023. Jusqu'en avril 2021, Microsoft Teams recensait le nombre de ses utilisateurs actifs quotidiens, et rapporte depuis juillet 2021 le nombre de ses utilisateurs actifs mensuels (REDMOND T., « Is Microsoft's Claimed 250 Million Teams Monthly Active Users Believable? », sur *Office365itpros.com*, 28 juil. 2021). Ainsi, mi 2021, Microsoft Teams comptait

en ligne Alipay bondit probablement de plus de 150 millions pour la première fois depuis son lancement en 2004, passant de 370-395 millions en 2019 à 515-545 millions en 2020¹⁰⁶³. La pandémie a aussi sans doute nettement contribué à l'essor de TikTok, de Telegram, à l'augmentation de la demande en smartphones (tant Android qu'Apple)...

Quelle que soit l'exception concernée, les bonds exceptionnels sont entraînés par un effet de réseau – l'utilité sociale d'une application augmente à mesure qu'augmente le nombre de ses utilisateurs actifs. Le plus souvent, une application assure une croissance à long terme de son MAU en combinant plusieurs exceptions ou en répétant plusieurs fois une même exception. Par exemple, le MAU Alipay n'aurait probablement pas bondi de plus de 150 millions sous l'effet de la pandémie (exception de crise/bouleversement) si cette application de paiement n'était pas déjà très bien insérée au fonctionnement et aux usages d'autres programmes très utilisés mondialement – les applications de commerce en ligne Alibaba, Tmall, TaoBao, Aliexpress... (exception d'insertion). Alipay a donc dû cumuler ces deux exceptions pour effectuer un bond de plus de 150 millions dans son histoire.

On trouve aussi des applications qui s'efforcent de combiner la première exception (exception fédératrice et nouvelle) avec la deuxième (exception d'insertion), de les répéter l'une et/ou l'autre pour bondir sur plusieurs années successives, comme Facebook, Google Search ou WeChat. Pour ne prendre que le cas de WeChat, on a vu que les fonctions nouvelles qu'il a popularisées (messagerie instantanée vocale et localisation des personnes à proximité) sur un support fédérateur et largement adopté (messagerie instantanée) ont fait les débuts de son succès. En plus de cette première exception, Tencent a joué très tôt sur la deuxième en permettant dès 2011 aux utilisateurs de QQ d'importer leurs contacts sur WeChat et inversement, après quoi des dizaines de millions d'internautes ont rejoint WeChat¹⁰⁶⁴. WeChat s'insère très bien avec les usages de QQ (réseau social le plus utilisé à l'époque, propriété de Tencent), et profite ainsi de sa base d'utilisateurs pour atteindre 50 millions en novembre 2011¹⁰⁶⁵. En 2012, Tencent fait à nouveau appel à la

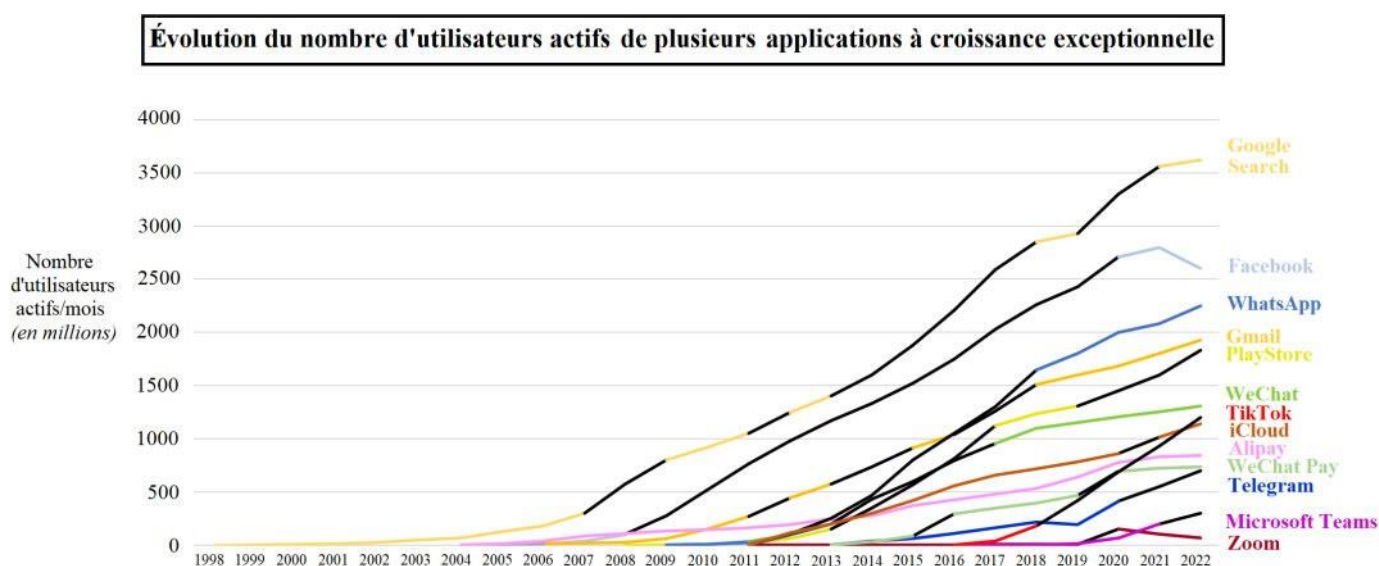
environ 250 millions d'utilisateurs actifs mensuels pour 145-150 millions d'utilisateurs actifs quotidiens – soit un ratio moyen d'1,65-1,75 utilisateur actif mensuel pour 1 utilisateur actif quotidien. On a évalué le MAU de Microsoft pour la période antérieure à avril 2021 à l'aide de ce ratio, en l'abaissant progressivement à 1,2-1,5 utilisateur mensuel/utilisateur quotidien pour juillet 2019 alors que Teams ne rassemblait que 13 millions d'utilisateurs actifs quotidiens (soit probablement 15-20 millions d'utilisateurs mensuels).

¹⁰⁶³ On a évalué le MAU d'Alipay selon : la part de marché qu'il représentait sur le marché chinois des moyens de paiement en ligne (TORRE Dominique, XU Qing, « Digital payments in China: adoption and interactions among applications », *Revue d'économie industrielle*, vol. 172, oct. 2020, p. 58) ; la taille du marché chinois des acheteurs et vendeurs en ligne en 2020 (SLOTTA Daniel, « Number of online payment users in China from 2011 to 1st half of 2022 », sur *Statista.com*, oct. 2022) ; et le nombre d'utilisateurs étrangers d'Alipay, qu'on a estimé selon des fourchettes basse et haute proportionnelles au nombre d'utilisateurs actifs étrangers des applications d'Alibaba (15-45 millions d'utilisateurs mensuels étrangers d'Alipay en 2019 pour 120 millions d'utilisateurs annuels étrangers d'Alibaba Group, 30-70 millions d'utilisateurs mensuels étrangers d'Alipay en 2020 pour 180 millions d'utilisateurs annuels étrangers d'Alibaba Group : v. MA Yihan, « Number of annual active consumers on Alibaba Holding Limited's overseas retail platforms from fiscal year 2019 to fiscal year 2022 », sur *Statista.com*, sept. 2022).

¹⁰⁶⁴ HARIHARAN Anu, « How WeChat Grew to Be the #1 App in the World », sur *Ycombinator.com*, 2017. YCombinator est un groupe d'investisseurs et conférenciers qui propose aux propriétaires de start-ups d'investir dans leur entreprise et de les former au lancement de leur start-up sur le marché. Cet article est bien documenté.

¹⁰⁶⁵ *Ibid.*

première exception en créant deux nouvelles fonctionnalités très populaires sur sa messagerie instantanée : la possibilité de créer des groupes de discussion exclusivement composés d'amis en commun (avec la fonctionnalité « Moments ») et de suivre à sens unique des célébrités internet pour recevoir régulièrement leur contenu (avec les « Official Accounts », suivis à sens unique d'une manière proche de ce qui peut se faire sur Twitter ou Weibo). En 2013, Tencent combine à nouveau l'exception fédératrice/nouvelle et l'exception d'insertion pour créer WeChat Pay, une application de paiement en ligne qui s'insère très bien avec les usages de WeChat. Nous n'avons pas identifié de bond exceptionnel du MAU WeChat Pay, mais on pense que cette application a pu contribuer aux bonds de WeChat en l'enrichissant d'une nouvelle fonction fédératrice et populaire (le paiement en ligne). On représente ainsi l'évolution de certaines applications dont le MAU a bondi de plus de 150 millions sur une année, en noircissant la courbe chaque année où elle fait un tel bond :



On tire deux leçons de ce schéma. On observe premièrement que chaque application dont le MAU a été supérieur à 500 millions a mis plusieurs années pour y parvenir : Google Search a mis 10 ans, Telegram plus de 7 ans, Facebook 6 ans, Play Store, WhatsApp et Gmail 6 ans, iCloud 4 ans, WeChat et TikTok 3 ans. **À un rythme constant supérieur à 250 millions chaque année (jamais vu jusqu'à présent), le MAU d'une application partant de zéro rattrapera en plus de 15 ans (vers 2037-2038) le niveau de Google Search de 2022.** Même les applications mondialement très utilisées (par plus de 100 millions de personnes) peuvent difficilement rivaliser avec Google Search.

Pour citer les croissances les plus spectaculaires, sachant qu'elles ont tendance à diminuer au fil du temps : le MAU de Facebook a une croissance moyenne de 155 millions chaque année sur dix-huit ans entre 2004 et 2022, celui de Play Store a une croissance moyenne de 190 millions sur 14 ans entre 2008 et 2022, celui de WhatsApp a une croissance moyenne de 180 millions chaque année sur treize ans entre 2009 et 2022, celui de TikTok/Douyin a une croissance moyenne de 196 millions chaque année sur six ans entre 2016 et 2022... **et le MAU de Google Search a une croissance moyenne de 200 millions chaque année sur dix-huit ans entre 2004 et 2022.** Ces données illustrent combien l'écart entre Google Search et les autres applications à croissance exceptionnelle restreint le marché. En 2022, très peu

d'applications à croissance exceptionnelle – et encore moins de nouvelles applications – peuvent atteindre le niveau de Google Search. Autrement dit, **plus se creuse l'écart entre le MAU de l'application dominante** (par ex. Google Search) **et le MAU des applications dominées**, plus il sera difficile pour les applications dominées de rattraper cet écart et d'accéder au niveau de l'application dominante, donc **plus le marché sera fermé** (difficulté d'alterner l'acteur dominant, par ex. Alphabet). Cela signifie que plus cet écart est important, plus se réduit l'échantillon de nouvelles applicables capables de devenir dominantes.

Ce schéma nous permet de faire une seconde observation. De plus en plus d'applications à croissance exceptionnelle s'insèrent avec d'autres programmes très utilisés mondialement. Google Search (MAU de 3,5-3,7 milliards), Chrome (MAU de 2,55-2,75 milliards), Play Store (MAU de 2,6-2,7 milliards) et Gmail (MAU de 1,8-1,9 milliards) sont très bien intégrées aux usages des smartphones Android, sachant que les smartphones Android connectent environ 2.25 milliards d'utilisateurs actifs fin 2022¹⁰⁶⁶. Ces applications sont alors alimentées par la base d'utilisateurs d'Android. De même, YouTube (MAU de 2,55-2,65 milliards), Google Maps (MAU de 1,35-1,55 milliards), Google Translate (MAU de 975 millions-1,15 milliard), Google Assistant (650-750 millions) et Google Ads (650-720 millions) s'insèrent très bien avec les usages faits de Google Search voire d'Android, ce qui fait des **applications d'Alphabet les plus centrales mondialement sur les marchés des moteurs de recherche** (Google Search), **des réseaux sociaux de partage de vidéos** (YouTube), **des boîtes de messagerie** (Gmail), **des magasins d'applications** (Play Store), **de la cartographie en ligne** (Google Maps), **de la publicité en ligne** (Google Ads et YouTube Ads), **de la traduction multilingue** (Google Translate), **des assistants intelligents** (Google Assistant) **et des systèmes d'exploitation** (Android, qui n'est pas une application en ligne mais un système d'exploitation).

Dès lors que la croissance des applications d'Alphabet s'appuie sur celle de ses programmes les plus utilisées mondialement – Google Search et Android –, ses applications sont privilégiées sur chaque segment de marché où elles surviennent par rapport aux autres applications. Outre l'écart entre les MAU, cette stratégie d'insertion est un deuxième facteur de fermeture du marché : les applications développées par Alphabet sur un segment de marché peuvent profiter de la base d'utilisateurs de Google Search et Android, et sont alors privilégiées par rapport aux autres applications de ce même segment pour bondir exceptionnellement, et ainsi creuser l'écart avec ces autres applications. C'est ce qu'on observe pour Play Store. Son insertion avec Android alimente son MAU à hauteur de 2,6-2,7 milliards, lui a assuré plusieurs bonds exceptionnels successifs entre 2013 et 2017 puis entre 2019 et 2022, et en a fait le premier magasin d'applications creusant de plus en plus l'écart avec le deuxième magasin d'applications (AppStore, MAU de 1,4-1,6 milliards, écart de plus d'un milliard d'utilisateurs actifs par mois avec Play Store, soit un écart de plus de sept ans au rythme moyen de croissance d'AppStore). AppStore lui-même doit sa deuxième place à son insertion avec les systèmes d'exploitation d'Apple, iOS (pour smartphones) et macOS (pour ordinateurs), qui sont les troisième et quatrième systèmes d'exploitation les plus utilisés dans le monde après Android et Windows¹⁰⁶⁷. Il en va de même pour iCloud, iMessage (messagerie instantanée, MAU de 1,1-1,25 milliards fin 2022) ou encore Siri

¹⁰⁶⁶ Soit 71,8% du marché des systèmes d'exploitation sur mobile dans le monde et 40.9% du marché global des systèmes d'exploitation (mobile + bureau) : LARICCHIA F. « Mobile operating systems' market share worldwide from 1st quarter 2009 to 4th quarter 2022 » sur *Statista.com*, janv. 2023 ; et TAYLOR Petroc, « Population of internet users worldwide from 2012 to 2021, by operating system », sur *Statista.com*, mai 2022

¹⁰⁶⁷ « Operating System Market Share Worldwide », *StatCounter*

(assistant vocal intelligent, MAU de 550-625 millions fin 2022), tous trois très bien insérés aux iPhones. Toutes ces applications profitent de la base d'utilisateurs actifs d'Apple, qu'on situe entre 1,3 et 1,5 milliards fin 2022. On a vu aussi que WeChat Pay est très bien inséré avec WeChat, et qu'Alipay est très bien inséré avec les différents services de commerce en ligne d'Alibaba. Contrairement aux « géants d'internet » (Alphabet, Apple, Meta...), les nouveaux arrivants sur le marché ne sont encore propriétaires d'aucun programme très utilisé mondialement et peuvent donc très difficilement s'insérer avec de tels programmes pour profiter de leur base d'utilisateurs. **Les applications des nouveaux arrivants sont alors fortement désavantagées par rapport aux nouvelles applications des géants d'internet, quant à elles privilégiées par leur insertion avec des programmes déjà très utilisés.**

Quasiment non encadrés aujourd'hui, ces deux facteurs de fermeture du marché (ampleur de l'écart entre les MAU des applications, et insertion des nouvelles applications des géants d'internet avec leurs programmes déjà très utilisés) s'accompagnent d'une centralisation croissante des applications en ligne par un petit nombre de gestionnaires (Paragraphe 2).

Paragraphe 2. Les centralités de gestion et de fonctionnement des applications en ligne

Tandis que la centralité de gestion des application amplifie leur centralité de connexion (A), le fonctionnement des applications s'est à son tour fortement centralisé depuis la fin des années 2000 (B).

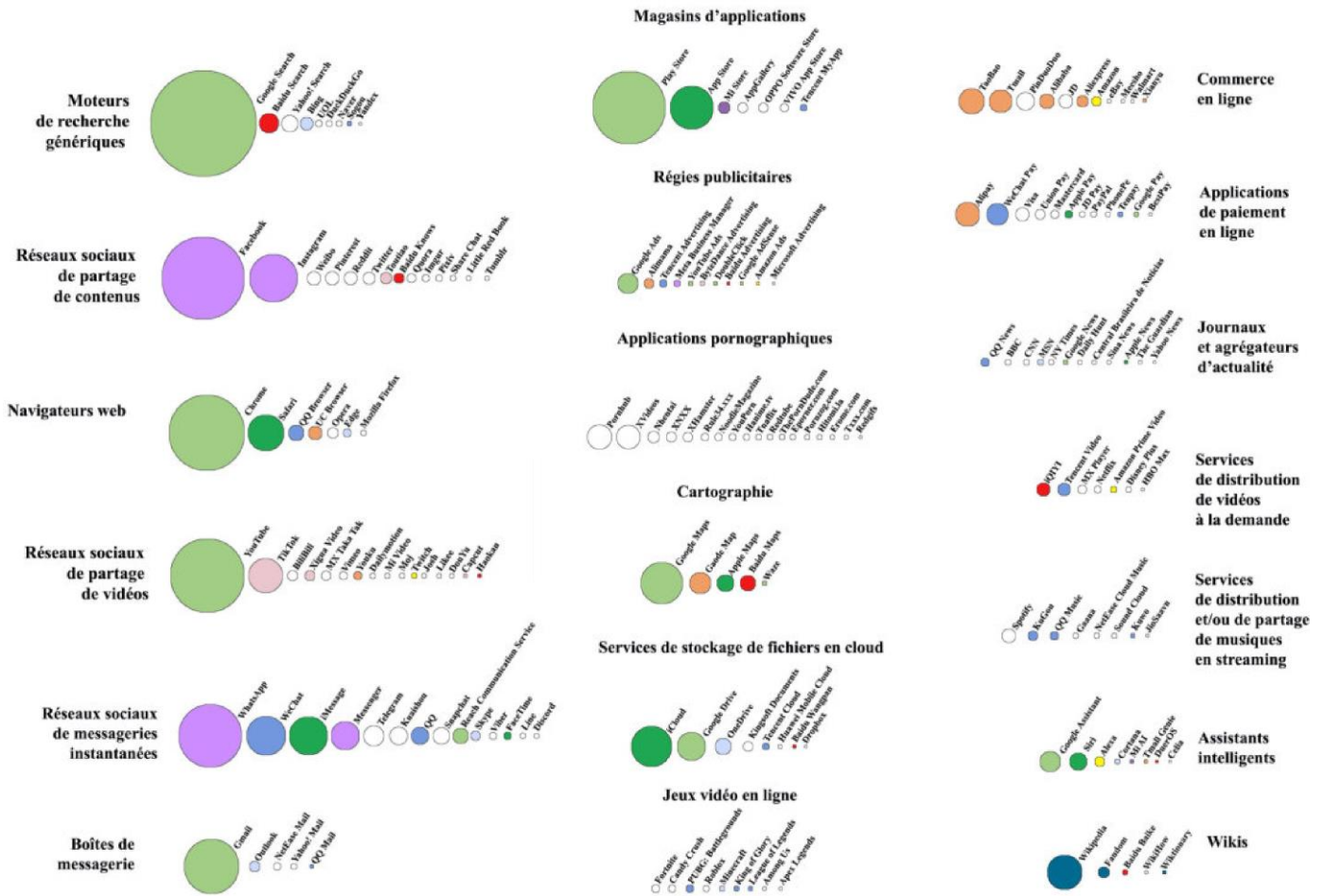
A) L'aggravation de la centralité de connexion par la centralité de gestion

1. L'appropriation des principaux segments de marché par les géants

On vient de constater que l'essor de certaines applications était privilégié du fait de leur insertion, ce qui a pour effet de creuser l'écart avec les autres applications, et donc de créer un retard très difficilement rattrapable pour ces applications moins bien insérées. Les géants d'internet peuvent ainsi reproduire leur domination à travers les générations, tant sur les segments de marché du Web 1.0 (moteurs de recherche, commerce en ligne, journaux et agrégateurs d'actualités, boîtes de messagerie, distribution de musiques en streaming, jeux vidéo en ligne, sites pornographiques, applications de paiement en ligne, cartographie en ligne, régies publicitaires) que sur ceux du Web 2.0 (réseaux sociaux de partage de contenus, de partage de vidéos, de messageries instantanées), du Web 3.0 (stockage de fichiers en cloud, magasins d'applications) voire du Web 4.0 (assistants vocaux intelligents)¹⁰⁶⁸. Tous ces segments marchés, anciens comme nouveaux, sont systématiquement investis puis dominés par les géants d'internet. On l'observe clairement sur ce schéma :

¹⁰⁶⁸ Le Web 1.0 (ou « Web traditionnel ») est un rétronyme qui désigne la période d'existence du Web entre 1989 et 2004 environ, jusqu'à l'essor du Web 2.0. Le Web 2.0 (ou « Web participatif ») couvre la période de 2004 à la première moitié des années 2010 et désigne la naissance d'applications dédiées aux interactions d'internautes (réseaux sociaux, forums, wikis...). Le Web 3.0 a débuté son essor vers la fin des années 2000 et possède deux composants, dont le Web sémantique d'après le fondateur du Web et président de l'Internet Society Tim Berners-Lee (OZARDE Sandeep, doctorant à l'université de Hertfordshire, « Tim Berners-Lee, Semantic Web 3.0 », sur *Linkedin*, 8 mai 2022). Le « Web sémantique » est caractérisé par un nouveau langage informatique – le Resource Description Framework – qui permet de traiter les données des internautes selon la signification littérale et non plus mathématique de ces données (par exemple, les moteurs de recherche proposent désormais les résultats selon la signification littérale des requêtes de l'utilisateur). Ce qu'on appellera le « Web synchronisé » (deuxième composant du Web 3.0) renvoie aux trois technologies popularisées au même moment consistant à synchroniser les données stockées par les différentes machines utilisée par l'internaute : la

Comparaison des applications de plus de 100 millions d'utilisateurs actifs/mois dans le monde au dernier semestre 2022 par segment de marché



Pour réaliser ce schéma, on s’est appuyé sur les MAU des différentes applications recensées en Annexe. La taille de chaque application varie proportionnellement à son MAU fin 2022. Les applications colorées sont celles qui appartiennent à des géants d’internet.

Premièrement, on observe que, **sur certains segments de marchés, l'écart** entre la première application et les applications suivantes **est particulièrement grand** : le segment des **moteurs de recherche** (dominé par Google Search), celui des **boîtes de messagerie** (dominé par Gmail), celui des **réseaux sociaux de partage de vidéos** (dominé par YouTube, qui n'a que TikTok pour concurrent menaçant), et celui des **applications pornographiques** (dominé doublement par

technologie cloud ; le smartphone ; et les objets connectés. On verra plus loin que les Web 2.0 et 3.0 ont eu un effet très centralisateur sur le fonctionnement d'internet. Par opposition, on parlera de Web 3.1 (ou « Web décentralisé ») pour désigner les technologies de décentralisation qui ont émergé dans la première moitié des années 2010 (VPN, blockchain, crypto-marchés utilisant les darknets pour des ventes illicites...). Le Web 3.1 nourrit les rêves du mouvement politique baptisé « Web3 », espérant voir un réseau de type internet dont le fonctionnement reposerait sur la technologie décentralisée de la blockchain (EDELMAN Gilad, « The Father of Web3 Wants You to Trust Less », *Wired*, nov. 2021). Enfin, le Web 4.0 (ou « Web intelligent ») a débuté son ascension dans la deuxième moitié des années 2010 et désigne le recours à l'intelligence artificielle pour des applications en ligne. Propulsé par les assistants vocaux des smartphones et des enceintes connectées (avec Siri né en 2011, Cortana et Alexa-Amazon Echo nés en 2014, Xiaodu Assistant né en 2015, Google Assistant né en 2016...), le Web 4.0 se voit en 2023 enrichi par de nouveaux types d'applications de plus en plus populaires (logiciels éditeurs d'images par IA, réseaux sociaux de partage d'images ou de vidéos créées par IA...).

Pornhub et XVideos). L'ampleur de ces écarts révèle que ces segments de marché sont assez voire très fermés – très peu d'applications ont le potentiel ou les moyens pour détrôner la première application.

Deuxièmement, d'autres segments de marché sont fermés par le fait qu'**une même entreprise possède plusieurs applications parmi les plus utilisés de ce segment** : le segment des **réseaux sociaux de partage de contenus** est largement dominé par deux applications (Facebook et Instagram) appartenant à Meta, et l'écart de ces applications avec les suivantes est difficilement rattrapable ; quant au segment des **services de commerce en ligne**, quatre des six applications les plus utilisées mondialement appartiennent à Alibaba (Taobao, Tmall, Alibaba et Aliexpress), et les autres services de commerce en ligne accusent un tel retard vis-à-vis des applications d'Alibaba que ces dernières sont difficilement détrônables sur ce segment.

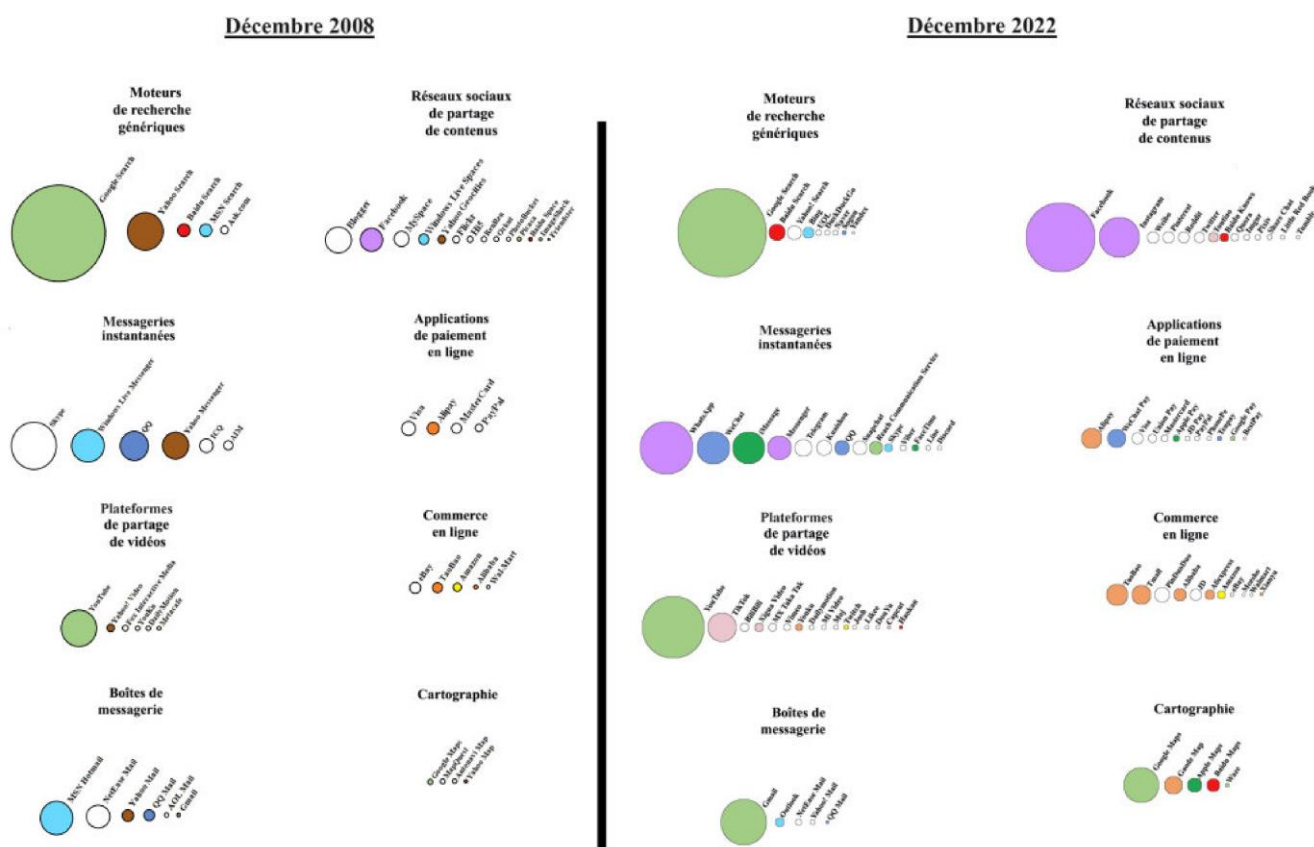
Troisièmement, d'autres segments ne semblent pas présenter d'écart spectaculaire mais sont accaparés par des géants d'internet : les quatre premières applications du segment des réseaux sociaux de messagerie instantanée appartiennent à des géants d'internet ; idem pour les quatre premières applications du segment des assistants intelligents ; quant aux segments des régies publicitaires et de la cartographie en ligne, toutes les applications dont le MAU est supérieur à 100 millions appartiennent à des géants d'internet. Concernant les assistants intelligents, précisons néanmoins qu'une application née le 30 novembre 2022 provoque une grosse secousse sur ce marché : l'application ChatGPT, développée par la start-up OpenAI à l'aide d'un investissement d'un milliard de dollars par Microsoft. Assistant textuel intelligent, ou encore « robot conversationnel », ChatGPT a gagné 100 millions d'utilisateurs actifs en moins de trois mois (entre fin décembre 2022 et début février 2023)¹⁰⁶⁹ – une croissance encore jamais atteinte par aucune application. N'ayant franchi le seuil des 100 millions que début 2023, ChatGPT ne figure néanmoins pas dans notre liste des applications en ligne les plus utilisées mondialement lors du dernier semestre 2022, et n'intègre donc pas notre schéma.

Quatrièmement, à l'exception du segment des jeux vidéo en ligne, tous les autres segments représentés sont dominés par un voire plusieurs géants d'internet. Sur presque tous les segments de marché, les applications des géants d'internet creusent l'écart avec les autres applications, ce qui ferme de plus en plus ces segments aux concurrents des géants d'internet. Quant aux jeux vidéo en ligne les plus utilisés mondialement, la moitié d'entre eux appartiennent à deux géants (Tencent et Microsoft).

Cinquièmement, la plupart des applications figurant sur ce schéma qui appartiennent à des géants ont fait l'objet soit d'une stratégie d'insertion avec d'autres programmes très utilisés mondialement (YouTube, Gmail, Play Store, Google Maps, Google Drive, Rich Communication Service et Google Assistant avec Google Search et Android, AppStore, iMessage, iCloud, Siri, FaceTime et ApplePay avec les systèmes d'exploitation d'Apple, WeChat avec QQ puis WeChat Pay, QQ News et Qzone en son temps avec WeChat et QQ, Baidu Maps, Baidu Baike, Baidu Knows et Baidu Wangpan avec Baidu Search et Baidu Browser, Bing, OneDrive, Skype et Cortana avec Windows et Edge, Alipay avec les applications de commerce en ligne d'Alibaba...), soit d'un rachat par un géant (WhatsApp, Instagram et FB Messenger rachetés par Meta, [Musical.ly](#) racheté par ByteDance et fusionné avec TikTok, Autonavi Map et Youku rachetés par Alibaba, YouTube racheté par Google, Twitch racheté par Amazon, iQIYI racheté par Baidu, Sogou racheté par Tencent, Skype racheté par Microsoft...).

¹⁰⁶⁹ MILMO Dan, « ChatGPT reaches 100 million users two months after launch », *The Guardian*, 2 fév. 2023 ; HU Krystal, « ChatGPT sets record for fastest-growing user base », *Reuters*, 2 fév. 2023

On constate ici clairement que **les géants d'internet maintiennent et démultiplient leur domination sur les différents segments de marché grâce à des stratégies d'insertion et des opérations de rachat des concurrents**, qui permettent à ces acteurs d'accroître leur présence sur ces marchés, de creuser l'écart avec les concurrents de ces géants, et donc de fermer la possibilité de se faire dépasser par ces concurrents. Autrement dit, **plus le temps avance, plus les géants assoient leur domination sur les différents segments de marché** à coups d'insertions-fusions et de rachats, et ferment ces marchés à la concurrence en se rendant indétrônables. Une comparaison avec l'état du marché en 2008 nous conduit à confirmer cette centralisation grandissante :



Pour connaître le MAU des applications en ligne en décembre 2008, on s'est principalement appuyé sur les études de comScore et d'iResearch menées à cette époque. En 2008, 1,7 milliards de personnes dans le monde étaient connectées à internet (contre 5,07 milliards en 2022). Google Search avait alors 725-750 millions d'utilisateurs actifs/mois¹⁰⁷⁰ (contre à peu près 3,5-3,6 milliards en 2022). On a réalisé le schéma de 2008 comme celui de 2022, *i.e.* en attribuant une taille 100 à l'application la plus utilisée mondialement (Google Search en 2008 comme en 2022), puis en faisant varier la taille des autres applications proportionnellement à la taille de Google Search d'après leur MAU respectif. Par ailleurs, pour qualifier une application comme étant « très utilisée mondialement » en 2008, on a abaissé le seuil proportionnellement au nombre d'internautes cette année-là (à 30 millions en 2008 au lieu de 100 millions en 2022). Ne figurent donc sur le schéma de 2008 que des applications dont le MAU dépassait 30 millions. Par exemple, fin 2008,

¹⁰⁷⁰ CATONE Josh, « comScore: Web Audience Now Tops 1 Billion », *Sitepoint.com*, 24 janv. 2009

QuestMap comptait 43 millions d'utilisateurs contre 41 millions pour Google Maps qui le dépassera en janvier 2009¹⁰⁷¹, Facebook totalisait 200 millions d'utilisateurs¹⁰⁷², TaoBao 55-75 millions¹⁰⁷³, YouTube 220-240 millions¹⁰⁷⁴.

Le marché était nettement moins fermé par les géants d'internet fin 2008 qu'en 2022. C'est frappant : aucun géant ne domine les segments des messageries instantanées, du partage de vidéos, des réseaux sociaux de partage de contenus, des moyens de paiement, du commerce en ligne, et le segment de la cartographie était dominé par QuestMap encore en juillet 2008. Plus encore, sur le segment du partage de contenus, le premier géant (Microsoft) n'arrive qu'en quatrième position, loin derrière les deux premiers – Facebook n'était alors pas encore un géant. On identifie sept géants mondiaux fin 2008, en définissant le « géant mondial » comme l'acteur qui connectait alors plus de 150 millions d'utilisateurs actifs/mois (soit 10% de la population mondiale d'internautes) et qui possédait au moins deux applications très utilisées mondialement : **Microsoft** (plus d'un milliard d'utilisateurs actifs/mois pour le navigateur Internet Explorer, environ 750 millions pour le système d'exploitation Windows, 287 millions pour MSN Hotmail, 275 millions pour Windows Live Messenger, 105 millions pour MSN Search, 87 millions pour Windows Live Space) ; **Google** devenu **Alphabet** (725-750 millions pour Google Search, 295 millions pour YouTube, 45 millions pour Picasa, 30 millions pour Gmail) ; **Yahoo** (375 millions pour Yahoo Search, 230 millions pour Yahoo Messenger, 99 millions pour Yahoo Mail, 69 millions pour Yahoo Heocities) ; **Tencent** (250 millions pour QQ, 110 millions pour Qzone, 97 millions pour QQ Mail) ; **Apple** (150-160 millions pour les systèmes d'exploitation d'Apple, 100 millions pour iTunes et probablement une centaine de millions pour Safari¹⁰⁷⁵) ; **Alibaba** (110 millions pour

¹⁰⁷¹ RAO Leena, « Trailing Google Maps, MapQuest Upgrades Developer Tools », *TechCrunch*, 12 oct. 2009

¹⁰⁷² SCHONFELD Erick, « Top Social Media Sites of 2008 (Facebook Still Rising) », *TechCrunch*, 31 déc. 2008

¹⁰⁷³ Pour un nombre d'utilisateurs annuels de 85 millions d'après les chiffres avancés par le propriétaire de l'application, Alibaba Group : WALRAVEN Piet, « A Brief History (and Future) of Alibaba.com », *Technode*, 22 janv. 2009 ; « Chinese Tech Stock Weekly Summary (Dec. 15 - 21, 2008) », *Seeking Alpha* [en ligne, entreprise d'analyse du marché technologique], 23 déc. 2008

¹⁰⁷⁴ Selon comScore, YouTube totalisait 158 millions d'utilisateurs uniques en janvier 2008, contre 181 millions en juin 2008, et un peu plus de 200 millions en août 2008 (respectivement ELDON Eric, « Roundup: YouTube making money now? Managers leaving Bebo, and more », sur *Venture Beat* [en ligne], 1^{er} juin 2008 ; et ANDO Ritsuko, « Mom joins trend of turning to YouTube for help », *NBC News* [en ligne], 1^{er} août 2008). Par ailleurs, le nombre d'utilisateurs américains de YouTube est passé de 80 millions en janvier 2008 à 92 millions en juillet 2008, puis à 120,5 millions en août 2009 (respectivement « YouTube.com Accounted for 1 Out of Every 3 U.S. Online Videos Viewed in January », *comScore* [en ligne], 14 mars 2008 ; « YouTube Draws 5 Billion U.S. Online Video Views in July 2008 », *comScore* [en ligne], 10 sept. 2008 ; et JARBOE Greg, « 120.5 million viewers watched nearly 10 billion videos on YouTube in August 2009 », *Search Engine Journal*, 28 sept. 2009). Compte tenu de la croissance moyenne du nombre d'utilisateurs de YouTube entre janvier et juillet 2008 (environ 4 millions de nouveaux utilisateurs uniques/mois), et de la croissance moyenne du nombre d'utilisateurs américains entre janvier 2008 et juillet 2009 (environ 2 millions de nouveaux utilisateurs uniques/mois entre janvier) puis entre juillet 2008 et août 2009 (environ 2,5 millions de nouveaux utilisateurs uniques/mois), on estime le MAU de YouTube entre 220 et 240 millions le nombre d'utilisateurs uniques de YouTube fin 2008

¹⁰⁷⁵ Concernant le nombre d'utilisateurs d'iTunes (logiciel de lecture et de gestion de musiques), v. l'étude de Nielsen Online d'avril 2008, recensée par « iTunes Player Hits a High Note, Passes RealPlayer », sur *Websiteoptimization.com*, 2008. Concernant le nombre d'utilisateurs des systèmes d'exploitation d'Apple cette année, une étude de NetMarketShare en janvier 2009 révélait que macOS

Alipay, 55-75 millions pour Taobao, 25-35 millions pour Alibaba) ; **Baidu** (155-185 millions pour Baidu Search, 40 millions pour Baidu Space)¹⁰⁷⁶ . Précisons que plusieurs organisations n'étaient pas loin de devenir des géants mondiaux : les géants chinois Alibaba (110 millions pour Alipay, 55-75 millions pour Taobao, 25-35 millions pour Alibaba) et NetEase (100-120 millions pour le portail web et boîte de messagerie 163.com, sachant que NetEase était aussi propriétaire du jeu vidéo en ligne le plus utilisé au monde Fantasy Westward Journey, qui connectait probablement 15-25 millions d'utilisateurs mensuels)¹⁰⁷⁷ ; la Wikimedia Foundation, dont l'encyclopédie collaborative Wikipédia était probablement consultée par 225-250 millions d'utilisateurs par mois, mais qui ne possédait à notre connaissance qu'une seule application très utilisée mondialement en 2008¹⁰⁷⁸ ; et les entreprises

possédait à cette époque 9,8% des parts de marché des systèmes d'exploitation, ce qui représentait à peu près 165 millions des 1,7 milliards d'internautes fin 2008 (« Mac OS X market share accelerates in 2008 », sur *Successfulsoftware.net*, janv. 2009). Par ailleurs, 12 millions de personnes étaient titulaires d'un iPhone en 2008 (v. SATRIA HADI Antonius, « The influence of product attribute, promotion mix, distribution channel, and price toward repurchase intention on iPhone », *Asian Management and Business Review*, vol. 1, 2021). On en déduit que les terminaux d'Apple comptaient entre 165 et 175 millions d'utilisateurs actifs en 2008. Quant au navigateur par défaut d'Apple (Safari), il couvrait 4% des parts de marché des navigateurs en 2008, ce qui représentait entre 60 et 70 millions des 1,7 milliards d'internautes fin 2008 (v. RICHTER Felix, « 5 Years After Launch, Chrome is on Top of the Browser World », sur *Statista.com*, sept. 2013). On s'est appuyé sur le même document pour évaluer le nombre d'utilisateurs d'Internet Explorer fin 2008, lequel détenait alors 69% des parts du marché mondial des navigateurs. Tout comme Internet Explorer et Windows, MacOS, iOS, iTunes et Safari sont des applications et programmes locaux et non des applications en ligne, raison pour laquelle ils ne figurent pas sur notre schéma représentant les applications en ligne.

¹⁰⁷⁶ Pour Baidu Space, v. SCHONFELD Erick, « Top Social Media Sites of 2008 (Facebook Still Rising) », *TechCrunch*, 31 déc. 2008. On a évalué le nombre d'utilisateurs de Baidu Search à partir des données suivantes : la Chine comptait environ 253 millions d'internautes en 2008 et 298 millions en janvier 2009, Baidu possédait 63% des parts de marché des moteurs de recherche sur le sol chinois en juillet 2008 puis 75,5% au dernier trimestre 2010, et son audience atteignait 59,5% de la totalité des internautes résidant en Chine en octobre 2008 (BARBOZA David, « China Surpasses U.S. in Number of Internet Users », *The New York Times* [en ligne] 26 juil. 2008 ; « China Internet users soar to 298 million », *Reuters*, 14 janv. 2009 ; SCHONFELD Erick, « Google vs. Microsoft-Yahoo vs. China: The Story in Charts », *SeekingAlpha* [en ligne], 18 mars 2008 ; sur les parts de marché de Baidu en 2010, v. données de l'agence chinoise d'analyse du commerce en ligne Enfodesk rapportées par le blog de NGUYEN Chandler, « Search Engine Market share by country Mar 2011 », *Chandlernguyen.com*, 13 mars 2011). Compte tenu du rythme moyen de croissance de Baidu et de son audience fin 2008, on en déduit que, fin 2008, Baidu Search comptait environ 55-65% de 280-290 millions d'internautes résidant en Chine, soit 155-185 millions d'utilisateurs.

¹⁰⁷⁷ Pour NetEase Mail (163.com), v. MEYER Michael, MICHAEL David C. et NETTESHEIM Christoph, « China's Digital Generations. The 570-Million-Hour Opportunity », *The Boston Consulting Group*, juil. 2008, p. 30 ; BERENGUER Inaki, SHIJUN Cai, LIANG Li, JING Liu et WANG Ningya, « E-commerce at Yunnan Lucky Air », *MIT Sloan School of Management* [en ligne], août 2008, p. 5. Pour Westward Journey : ce jeu vidéo a obtenu le record du plus grand nombre de joueurs connectés simultanément en 2008, soit un pic de 1,66 millions de joueurs simultanés, légèrement devant World of Warcraft qui comptait 12 millions d'utilisateurs mensuels en 2008 (« Most users simultaneously online in an MMORPG », *Guinness World Records* [en ligne], consulté le 6 juin 2023). En 2008, la Chine comptait annuellement 50-58 millions de joueurs en ligne en 2008 d'après l'agence chinoise d'étude du marché technologique chinois Niko Partners (TAKAHASHI Dean, « Updated: Chinese online game market forecast to more than triple in five years », *Venture Beat* [en ligne], 2 mai 2008).

¹⁰⁷⁸ Fin 2009, il comptait environ 325 millions de visiteurs mensuels pour environ 600 millions de pages vues/mois ; fin 2011, il rassemblait 470 millions de visiteurs mensuels pour environ 800

américaines Facebook et Amazon, dont les applications éponymes comptaient alors respectivement 200 millions et d'utilisateurs et 65-85 millions d'utilisateurs¹⁰⁷⁹, mais qui elles aussi ne détenaient qu'une seule application très utilisée mondialement.

2. Conclusion sur la centralisation de gestion des applications en ligne entre 2008 et 2022

Depuis 2008, on a vu émerger quatre nouveaux géants mondiaux. En définissant le « géant mondial » de 2022 comme l'acteur qui connectait alors plus de 550 millions d'utilisateurs actifs/mois (soit 10% de la population mondiale d'internautes) et qui possédait au moins quatre applications très utilisées mondialement sur au moins deux segments de marché, on identifie les nouveaux géants suivants : Meta (ex-Facebook), Wikimedia Foundation, ByteDance et Amazon. Contrairement aux trois autres, Wikimedia Foundation est une organisation à but non lucratif, mais certaines de ses filiales sont lucratives, comme sa filiale Fandom Inc. propriétaire des applications très utilisées Fandom et [Gamespot.com](https://www.gamespot.com). On classe ainsi les **géants des applications fin 2022**, du plus au moins important par leur audience mensuelle : **Alphabet** (3,5-3,7 milliards pour Google Search, 2,8-3,1 milliards pour le système d'exploitation Android, 2,55-2,75 milliards pour le navigateur Chrome, 2,45-2,65 milliard pour Play Store, 2,3-2,6 milliards pour YouTube, 1,8-2 milliards pour Gmail, 1,35-1,55 milliards pour Google Maps, 975 millions-1,15 milliard pour Google Translate, 950 millions-1,05 milliard pour Google Drive, 650-750 millions pour Google Assistant, 500-545 millions pour Rich Communication Service, 155-170 millions pour Google Play, 151 millions pour Waze, 140-160 millions pour Google News) ; **Meta** (2,7-2,9 milliards pour Facebook, 2,1-2,3 milliards pour WhatsApp, 1,5-1,7 milliards pour Instagram, 920-960 millions pour Messenger) ; **Microsoft** (1,7-1,75 milliards pour le système d'exploitation Windows, 500-600 millions pour OneDrive, 400-425 millions pour Bing, 347 millions pour Outlook, 300-310 millions pour Skype, 270-280 millions pour Microsoft Teams, 225-285 millions pour le navigateur Edge, 200 millions pour LinkedIn, 195 millions pour MSN, 173 millions pour Minecraft, 145-160 millions pour Cortana) ; **Tencent** (1,3-1,4 milliards pour WeChat, 715-760 millions pour WeChat Pay, 574 millions pour QQ, 435-450 millions pour Tencent Video, 309 millions pour KuGou, 275 millions pour QQ Music, 250-290 millions pour QQ News, 238 millions pour PUBG Battlegrounds, 135-145 millions pour Sogou, 222-230 millions pour QQ Mail, 160-260 millions pour Tencent MyApp, 200-210 millions pour Tencent Docs, 160-175 millions pour Tenpay, 154 millions pour King of Glory, 150 millions pour Kuwo, 148 millions pour League of Legends, 135-145 millions pour Sogou, 111 millions pour WeChat Work, 100-110 millions pour Tencent WiFi Manager) ; **Apple** (1,25-1,35 milliards pour les systèmes d'exploitation macOS et iOS, 1,08-1,18 milliards pour iCloud, 975 millions-1,015 milliard pour AppStore, 935-965 millions pour le navigateur Safari, 900-950 millions pour iMessage, 550-625 millions pour Siri, 210-280 millions pour Apple Pay, 200-275 millions pour FaceTime, 225 millions pour Shazam) ; **Wikimedia Foundation** (1,1-1,3 milliard pour Wikipedia, 350-375 millions pour Fandom, 107 millions pour Wiktionary, 103 millions pour [Gamespot.com](https://www.gamespot.com)) ; **Alibaba** (870-930 millions pour Alipay, 875 millions pour Taobao, 780 millions pour Tmall, 730 millions pour Autonavi Map, 493 millions pour Alibaba, 373

millions de pages vues/mois ; avec ses 450 millions de pages vues/mois fin 2008, on estime le MAU de Wikipédia entre 225 et 250 millions : ANGWIN Julia, « Wikipédia connaît une crise de croissance », *Courrier International*, 9 déc. 2009 ; KOCH Simon, « Dons – Les Suisses sont les plus généreux avec Wikipédia », *Tribune de Genève*, 3 janv. 2012 ; et, pour l'évolution du nombre de pages vues/mois, v. les statistiques officielles de la Wikimedia Foundation rapportées par le blog du doctorant MOORE Benjamin, « Wikipedia is dead, long live the 'pedia », sur benjaminmoore.wordpress.com, 9 janv. 2014

¹⁰⁷⁹ Amazon détenait 72 millions de clients mensuels en janvier 2008, contre 114 millions au premier semestre 2010 : BÉGHIN Frédéric, « Jef Bezos, fondateur et PDG d'Amazon : "Pour innover, il faut ignorer les résultats à court terme" », *Capital*, 28 janv. 2008 ; VERCESI Patrick, « Amazon installe une base logistique à Montélimar », *Les Échos*, 1^{er} juil. 2010. Au rythme moyen de croissance d'Amazon entre janvier 2008 et mi-2010, on estime le nombre d'utilisateurs mensuels d'Amazon à 65-85 millions fin 2008

millions pour Aliexpress, 200-275 millions pour Youku, 225 millions pour DingTalk, 90-130 millions pour Tmall Genie) ; **ByteDance** (1,1-1,175 milliards pour TikTok, 350-380 millions pour TouTiao, 325 millions pour Xigua Video, 100-125 millions pour Capcut, 109 millions pour Fanqie Novel) ; **Baidu** (640 millions pour Baidu Search, 521 millions pour Baidu Maps, 415-465 millions pour iQIYI, 300-350 millions pour Baidu Knows, 275- 325 millions pour Baidu Baike, 110 millions pour Haokan, 104 millions pour Baidu Wangpan, 80-115 millions pour Xiaodu Assistant).

On voit **deux autres** acteurs qui sont proches d’être des géants des applications en ligne sur le plan de leur audience mensuelle, voire qui sont qualifiables comme tels sur le plan de leurs revenus, mais surtout qui sont des **géants d’internet** sur d’autres segments de marché que les applications : **Amazon** est le deuxième acteur dominant mondialement sur le segment de l’hébergement cloud, en plus de posséder cinq applications en ligne très utilisées mondialement (la place de marché la plus utilisée en Occident Amazon et ses 305-310 millions de clients mensuels, le plus grand service mondial de streaming de jeux vidéos Twitch et ses 325-331 millions d’utilisateurs actifs mensuels, 300-345 millions d’utilisateurs pour l’assistant vocal Alexa, 190-210 millions pour IMDb, 200 millions pour Amazon Prime Video) ; enfin, **Xiaomi** est le troisième fabricant mondial de smartphones par le nombre de ses ventes après Apple puis Samsung¹⁰⁸⁰, en plus de détenir quatre applications en ligne très utilisées mondialement (350-420 millions d’utilisateurs mensuels pour le magasin d’applications MiStore, 170-190 millions pour Mi Game Center, 160-190 millions pour le réseau social de partage de vidéos Mi Video, et 105-125 millions pour l’assistant vocal Mi AI)¹⁰⁸¹.

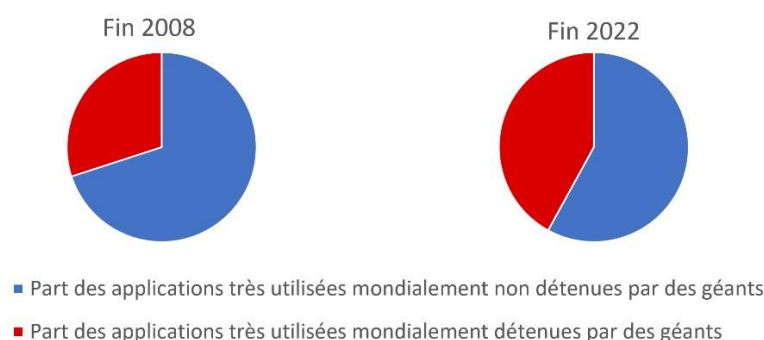
Les données qu’on a rapportées laissent voir une **forte centralisation des applications en ligne du fait de leur gestion**. On se concentrera ici sur les 255 applications que la marge d’erreur de notre estimation situe en toute hypothèse au-dessus de 100 millions. En nous référant à notre liste des applications les plus utilisées, on relève d’abord une très faible diversité de la nationalité des gestionnaires de ces 255 applications : plus de 78% des applications en ligne très utilisées mondialement appartiennent à des gestionnaires américains (46,3%) ou chinois (31,7%). Surtout, les **onze géants** des applications en ligne de 2022 (Alphabet, Meta, Microsoft, Tencent, Apple, Wikimedia, Alibaba, ByteDance, Baidu, Amazon et Xiaomi) **possèdent** à eux seuls 105 – soit **plus de 41% – de ces 255 applications en ligne très utilisées mondialement** fin 2022. Par comparaison, on estime que les sept géants de 2008 détenaient alors 28 à 33% des applications en ligne très utilisées mondialement. La comparaison avec 2008 révèle alors que

¹⁰⁸⁰ LARICCHIA Federica, « Global smartphone market share from 4th quarter 2009 to 1st quarter 2023 », *Statista*, 24 mai 2023

¹⁰⁸¹ Bien que Huawei ait fait une percée spectaculaire à la fin des années 2010, les sanctions américaines ont bloqué les ventes de smartphones Huawei en Occident, ce qui a empêché l’entreprise chinoise de se qualifier durablement comme « géant des applications ». Alors qu’il était le fabricant dominant de câbles sous-marin en Chine, Huawei dû vendre la majorité de ses parts de Huawei Marine Network en 2019 sous la pression des sanctions américaines (MANIÈRE Pierre, « Câbles sous-marins : Huawei jette l’éponge », *La Tribune*, 4 juin 2019). Nous n’avons identifié que trois applications en ligne très utilisées mondialement appartenant à Huawei : on estime à 370-410 millions le nombre d’utilisateurs d’appareils Huawei fin 2022, avec 315-350 millions d’utilisateurs par mois du magasin d’applications AppGallery, 100-170 millions pour le service de stockage de fichiers en cloud Huawei Mobile Cloud, et 60-100 millions pour l’assistant vocal Celia. Ces estimations pour Huawei et Xiaomi reposent principalement sur l’évolution du nombre de ventes de smartphones Huawei et Xiaomi dans le monde depuis 2008, sur les parts de marché des systèmes d’exploitation mobile détenues par Huawei et Xiaomi dans les pays où elles sont présentes, sur l’évolution du nombre de téléchargements des services de stockage de fichiers en cloud et des assistants intelligents, et sur le pourcentage de la population utilisant des assistants vocaux dans chaque pays. Il est possible que nous soyons passé à côté de certaines applications en ligne très utilisées de Huawei.

les applications très utilisées mondialement sont de plus en plus concentrées par un petit nombre de gestionnaires. Le fait qu'un grand nombre d'applications était très utilisé mondialement en 2022 par rapport à 2008 n'est pas le signe d'une plus forte décentralisation, mais d'une internationalisation des usages en ligne et d'un accroissement de l'accessibilité d'internet dans chaque pays. Les applications peuvent acquérir une très vaste audience à l'étranger, bien plus en 2022 qu'en 2008, favorisant ainsi l'apparition d'applications centrales mondialement.

Appropriation des applications très utilisées mondialement
par des géants



En somme, les applications en ligne sont bien plus centralisées en 2022 qu'elles l'étaient en 2008, sur le plan tant de leur connexion (écart de plus en plus difficilement rattrapable entre le MAU des dernières applications très utilisées et le MAU des premières applications très utilisées sur un même segment de marché) que de leur gestion (concentration des applications les plus utilisées mondialement par des géants d'internet, domination de tous les segments de marché par des géants). On explique cette double centralisation par les stratégies d'insertion et les rachats, qui enferment le marché dans un cercle vicieux. Les stratégies d'insertion privilégient l'essor des applications développées par les géants au détriment des « non géants ». Quant aux rachats, par des géants, d'applications déjà très utilisées ou en plein essor (par ex. YouTube racheté par Alphabet, WhatsApp par Meta, [Musical.ly](https://www.musical.ly/) par ByteDance), ils ont pour effet d'évincer la concurrence sur un segment de marché tout en amplifiant la présence des géants sur ce segment. Dans les deux cas, par insertion ou par rachat, les géants creusent l'écart avec les non géants, ce qui offre aux premiers de dominer chaque segment de marché. Autrement dit, **tant que des géants peuvent librement recourir à la stratégie d'insertion ou racheter des applications concurrentes, les segments de marché ne cesseront de se fermer de plus en plus**, creusant l'écart avec les plus petites applications, démultipliant la présence des géants en tête des segments de marchés, concentrant les applications les plus utilisées mondialement entre les mains des géants et réduisant les chances des non géants de dépasser les géants.

Faute de limites économiques et juridiques posées aux stratégies d'insertion et aux opérations de rachat sur les différents segments de marché, la centralisation de connexion et de gestion des applications se renforce au fil des ans¹⁰⁸². À défaut de telles limites, l'effondrement de géants profite à de nouveaux géants et à une concentration croissante des applications en

¹⁰⁸² Récemment, la Commission européenne vient par exemple d'autoriser le rachat par Microsoft de la très grande entreprise de jeux vidéo Blizzard, malgré le refus en première instance de l'autorité de la concurrence britannique (Competition and Markets Authority, « Anticipated acquisition by Microsoft of Activision Blizzard, Inc. », 26 avr. 2023)

ligne. En effet, plusieurs géants des applications en ligne se sont effondrés depuis la naissance d'internet – AOL depuis la moitié des années 2000, Qihoo360 et Yahoo depuis les années 2010, Huawei depuis la fin des années 2010 sous l'effet des sanctions américaines... Malgré ces effondrements, de nouveaux géants ont germé, certes plus nombreux et diversifiés, mais au détriment des non géants qui possèdent une part de plus en plus étroite des applications très utilisées mondialement. Quand bien même les géants actuels seraient dépassés à l'avenir, le scénario se répéterait : les acteurs dont les applications dépasseront celles des géants y inséreront leurs prochaines applications et/ou rachèteront des applications concurrentes, faisant de ces acteurs de nouveaux géants qui auront détrôné les précédents en devenant à leur tour des géants. Une ère de géants succèdera à une autre, condamnant ainsi le marché des applications dans une configuration toujours plus centralisée et fermée à la concurrence faute de limites économiques et juridiques. Les stratégies d'insertion et de rachat ont ainsi permis aux propriétaires d'applications en ligne les plus populaires depuis 2008 (Alphabet, Apple, Microsoft, Tencent, Meta, Alibaba, Baidu) de conserver leur domination malgré les bouleversements technologiques survenus depuis 2008 – expansion des réseaux sociaux, de l'hébergement cloud, des usages internet mobiles (notamment avec le smartphone), et de l'intelligence artificielle. La plupart de ces entreprises ont consolidé leur puissance sur ces nouveaux segments des réseaux sociaux (Tencent avec WeChat, Apple avec iMessage et FaceTime, Alphabet avec YouTube et Blogger), des smartphones (Alphabet avec Android, Apple avec iOS), de l'intelligence artificielle (Alphabet avec Google Assistant, Apple avec Siri, Baidu avec Xiaodu Assistant, Microsoft avec Cortana), du stockage en cloud de fichiers d'utilisateurs (Apple avec iCloud, Alphabet avec Google Drive, Microsoft avec OneDrive, Tencent avec Tencent Cloud) et de l'hébergement en cloud d'applications (Amazon, Alphabet, Apple, Alibaba, Microsoft, Tencent comme on le verra plus loin).

On en déduit que, faute de régulation des stratégies d'insertion, de rachat et d'omniprésence des agents économiques sur les segments de marché des applications, **le libre jeu concurrentiel a un effet centralisateur sur la gestion des applications et sur le nombre d'internautes qu'elles connectent**. Cela se traduit par le fait que, d'une part, de moins en moins d'applications sont capables de détrôner celles des géants sur le moindre segment de marché et, d'autre part, les internautes sont sans cesse plus concentrés par les géants mondiaux via leurs applications. En d'autres termes, le libre jeu concurrentiel ne permet pas, à lui seul, de provoquer une alternance de la domination des géants d'internet – ou alors à très long terme. Dès lors que **les stratégies d'insertion et de rachat** ne sont accessibles/efficaces que pour les entreprises déjà dotées d'une vaste base d'utilisateurs et de moyens financiers conséquents, de telles stratégies **constituent un privilège concurrentiel bénéficiant aux applications d'entreprises déjà très importantes sur le marché**. En favorisant excessivement l'essor des applications des très grandes plateformes sur l'essor des applications concurrentes, ce privilège concurrentiel mine les conditions d'égale concurrence de façon non négligeable.

Par son effet, un tel privilège concurrentiel contredit les fondements du droit de la concurrence. Le principe de libre concurrence est juridiquement indissociable de l'égal accès au marché¹⁰⁸³. Dans l'Union européenne, cette indissociabilité est rappelée par l'avocat général

¹⁰⁸³ Claire Mongouachon le résume très bien : « *La libre concurrence correspond à la liberté de chacun de prendre part au marché. Le marché n'étant jamais organisé que dans un cadre défini par la puissance publique, cette liberté n'est pas absolue, mais protégée traditionnellement par (...) la liberté d'entreprendre (...) ou les libertés de circulation (...). L'égale concurrence correspond à la*

Miguel Poiars Maduro : l' « objectif » du droit européen de la concurrence est « d'assurer, entre les États membres, la libre circulation des marchandises, des services, des personnes et des capitaux », et cet objectif est atteint en « accordant aux acteurs (...) le pouvoir de contester certaines entraves et la possibilité de se faire concurrence à armes égales »¹⁰⁸⁴. Cette égalité des armes concurrentielles est soulignée par le Service de recherche du Parlement européen, « la politique de concurrence de l'Union européenne (...) garantit que les entreprises puissent se faire concurrence sur un pied d'égalité sur les marchés de l'ensemble des États membres »¹⁰⁸⁵. On a vu aussi que le projet du Digital Market Act européen est soucieux d'interdire aux « contrôleurs d'accès » de privilégier ses services sur ceux des concurrents.

Aux États-Unis, le Département de la justice considère que « l'objectif des lois antitrust est de protéger la liberté et les opportunités économiques en favorisant une concurrence libre et équitable sur le marché. (...) La concurrence donne aux entreprises la possibilité de se battre sur les prix et la qualité, dans un marché ouvert et sur un pied d'égalité, sans être gênées par des restrictions anticoncurrentielles. »¹⁰⁸⁶. Dès 1914, le Clayton Antitrust Act tente d'égaliser les conditions de concurrence en interdisant les « directions imbriquées » (le fait pour une même personne de diriger plusieurs entreprises concurrentes), et les concentrations d'entreprises (fusions et acquisitions) « lorsqu'elles peuvent avoir pour effet de réduire sensiblement la concurrence »¹⁰⁸⁷. Cette législation n'a pas empêché Meta d'acquérir WhatsApp, Instagram et Beluga (devenu Messenger) qui sont parmi les réseaux sociaux les plus utilisés au monde, ni Alphabet d'acquérir YouTube, Blogger et son concurrent direct Waze (sur le segment de la cartographie en ligne), ni Microsoft d'acquérir Skype et Minecraft (5^e jeu vidéo en ligne le plus utilisé au monde), ni Amazon d'acquérir Twitch (7^e réseau social de partage de vidéos le plus utilisé) et IMDb (50^e application la plus utilisée au monde).

En Chine, la loi Anti-Monopole de 2008 interdit à son tour « la concentration d'entreprises qui entraîne, ou peut entraîner, l'élimination ou la restriction de la concurrence [sur le marché intérieur chinois] »¹⁰⁸⁸. Cette règle n'a pas non plus empêché Baidu d'acquérir iQIYI (plateforme de vidéos à la demande la plus utilisée au monde), ni Tencent d'acquérir KuGou (2^e application de distribution de musique en streaming la plus utilisée au monde), Kuwo (3^e application de distribution de musique en streaming la plus utilisée en Chine) et Sogou (2^e moteur de recherche le plus utilisé en Chine), ni Alibaba d'acquérir Autonavi Map (2^e service de cartographie le plus utilisé au monde et 1^{er} en Chine), UC Browser (navigateur web le plus utilisé en Chine) et YouKu (5^e réseau social de partage de vidéos le plus utilisé en Chine) ; tout comme elle n'a pas empêché Alibaba de cadencer le segment du commerce en

possibilité donnée à chaque opérateur de pouvoir se faire concurrence. Ainsi, pour que la libre concurrence soit offerte à chacun, elle devra être corrigée par les autorités publiques : il s'agit de limiter la liberté des opérateurs économiques afin que la puissance d'action des uns ne s'exerce pas au désavantage des autres. » (MONGOUACHON C., « Principe d'égalité et concurrence dans la jurisprudence du Conseil constitutionnel », *La Revue des Droits de l'Homme*, 2017 p.43)

¹⁰⁸⁴ Conclusions de M. Poiars Maduro, §33 sous CJCE, *Viking*, 11 décembre 2007, aff. C-438/05

¹⁰⁸⁵ SZCZEPAŃSKI Marcin, « Politique de concurrence de l'Union européenne. La clé d'un marché unique équitable », *Service de recherche du Parlement européenne*, oct. 2019, p. 39 : « La Commission [européenne] soutient fermement son point de vue de longue date selon lequel la compétitivité est améliorée grâce à (...) une concurrence basée sur le mérite, qui doit être ouverte et se dérouler sur un pied d'égalité »

¹⁰⁸⁶ [Justice.gov/mission](https://www.justice.gov/mission)

¹⁰⁸⁷ Clayton Act du 15 oct. 1914, Sections 7 et 8

¹⁰⁸⁸ Loi Anti-Monopole de la République populaire de Chine du 1^{er} août 2008, art. 3 (3)

ligne en y concentrant cinq applications concurrentes (Taobao, Tmall, Alibaba, Aliexpress et Xianyu) pour diminuer les chances des concurrents, ni ByteDance de pratiquer la même stratégie sur le segment du partage de courtes vidéos (avec les applications concurrentes TikTok, Xigua Video et Capcut).

En 2022, les stratégies d'insertion et de rachats ont rendu quasiment impossible l'égalité des chances entre concurrents. De la même manière que les rachats ou la concentration d'applications concurrentes sur un même segment de marché, on pense que les stratégies d'insertion doivent donc être appréhendées par le droit de la concurrence comme un privilège concurrentiel qui favorise excessivement l'essor des géants¹⁰⁸⁹. À moins qu'une technologie décentralisatrice se propage très rapidement auprès des internautes, une décentralisation à long terme ne peut survenir qu'en redéfinissant les règles concurrentielles pour limiter sérieusement le recours à l'insertion et aux rachats ainsi que la présence d'un même acteur sur plusieurs segments de marchés. Diverses mesures peuvent contenir l'expansion des agents économiques sur le marché des applications – obliger un propriétaire d'applications à choisir d'investir un seul des cinq principaux segments de marché (systèmes d'exploitation, moteurs de recherche, navigateurs web, magasins d'applications, réseaux sociaux), lui interdire de concentrer plus de deux applications concurrentes sur un même segment de marché, lui interdire d'insérer entre elles deux de ses applications sur un même segment de marché et plus de deux de ses applications sur des segments différents sauf sur obligation légale, obliger le fabricant du terminal et le concepteur du système d'exploitation à proposer à l'utilisateur de choisir entre plusieurs programmes concurrents (au moins huit moteurs de recherche, navigateurs web, suite bureautique, boîtes de messagerie le cas échéant...) dès la première configuration du système d'exploitation par l'utilisateur, ou encore prohiber le rachat d'une application couramment ou très utilisée mondialement lorsque le repreneur est propriétaire d'applications dont le MAU dépasse déjà 500 millions (seuil évolutif selon l'état du marché). De telles règles pourraient donner naissance à une multitude de grands ou moyens acteurs sur les différents segments de marché plutôt qu'à un petit nombre de géants qui accapare tous les segments. Quelles que soient les règles retenues, un encadrement des stratégies d'insertion, de rachat et d'omniprésence ne peut néanmoins garantir des conditions égales de concurrence que si tous les concurrents y sont mondialement contraints, *i.e.* si ces règles sont décidées au niveau international.

B) La centralité de fonctionnement des applications en ligne

On a évalué la centralité de connexion d'un nœud d'après le nombre de nœuds émetteurs ou destinataires qu'il connecte (nombre adresses IP connectées par un AS, nombre d'utilisateurs actifs connectés par une application, nombre de noms de domaine connectés par un service DNS). On a par ailleurs évalué la centralité de gestion d'un nœud d'après le nombre de nœuds tiers ayant le même propriétaire que le nœud dont la centralité est évaluée (nombre de câbles sous-marins, d'AS, de serveurs DNS ou encore d'applications qui ont le même propriétaire). On évalue enfin la centralité de fonctionnement d'un nœud d'après le nombre des nœuds tiers qui assurent la même fonction que celle assurée par le premier nœud. Moins il existe de nœuds tiers pour suppléer la fonction assurée par le premier nœud, plus ce nœud est centralisé par son fonctionnement. Inversement, plus la fonction assurée par le premier nœud peut être suppléée par d'autres nœuds, plus le premier nœud est décentralisé par son fonctionnement. Pour donner un exemple de

¹⁰⁸⁹ On rappelle avoir défini les stratégies d'insertion comme les pratiques qui consistent, pour un opérateur économique, à insérer l'une des applications qu'il détient avec le fonctionnement ou l'usage d'un de ses programmes très utilisé mondialement

décentralisation par le fonctionnement des noms de domaine, on a vu que les serveurs racine obéissent à un système anycast, grâce auquel une multitude de serveurs racine assurant la même fonction (traitement de toute requête DNS destinée à un TLD) peuvent prendre le relai des serveurs racine défaillants. Si, au contraire, un seul serveur racine assurait à lui seul cette fonction, ce nœud – et le réseau DNS racine avec – serait extrêmement centralisé par son fonctionnement.

On étudie ici l'exemple d'une technologie qui centralise fortement le fonctionnement de la plupart des applications depuis les années 2000 : la technologie cloud, qui est un mode d'hébergement des données. Pour comprendre cette technologie, précisons comment une application est hébergée en ligne. Toute application en ligne est constituée de divers fichiers tels que : les éléments d'architecture graphique (haut et bas d'une page web, structure de la page, logo de l'application, menu, colonnes, texte de présentation, espaces réservés aux publicités...) ; les fonctionnalités à disposition des utilisateurs (commentaires, likes, partage de contenus, actions dans un jeu vidéo...) ; les contenus (textes, images, vidéos, audios...) ; le(s) nom(s) de domaine de l'application (pour permettre à l'utilisateur d'accéder à l'application) ; les bases de données (qui répertorient et classent les différents onglets, pages web, données utilisateur, contenus, fonctionnalités...) ; les processus d'échanges de données entre programmes (renvoi d'une requête utilisateur vers une base de données pour permettre à l'internaute d'accéder aux onglets, pages et fonctionnalités de l'application, à ses données utilisateur... répertoriés dans la base de données, et logiciel dit « middleware » pour assurer la communication entre des systèmes, des fonctions isolées et des applications tierces) ; le cas échéant, les programmes de gestion des contenus (pour permettre au propriétaire de l'application de créer et d'éditer son site web à l'aide des outils proposés par le programme), de gestion de la relation client (CRM pour *Customer relationship management*, pour créer des canaux d'échanges avec les clients, automatiser les processus d'échanges avec les clients et analyser les informations échangées), de gestion intégrée (pour automatiser les tâches d'une entreprise comme la gestion des ressources humaines, la comptabilité, l'aide à la décision, la vente, la distribution, l'approvisionnement...), de surveillance réseau (pour vérifier le bon fonctionnement du/des serveur(s) qui hébergent l'application, la qualité et la quantité du trafic) et autres algorithmes de traitement de données (d'analyse des données personnelles, de prédiction, de modération, de tri, de valorisation, de validation...) etc. Tous ces fichiers sont stockés (« hébergés ») sur des serveurs, assurant ainsi à une application son existence en ligne.

Il existe aujourd'hui quatre modes d'hébergement d'une application, c'est-à-dire que le propriétaire d'une application possède quatre options pour héberger son application en ligne. Il peut d'abord réserver tout l'espace mémoire d'un serveur physique pour y héberger exclusivement son application, dans le cadre d'un hébergement dédié (*dedicated hosting*, solution coûteuse). Si son application ne nécessite pas un vaste espace mémoire, le propriétaire peut réserver seulement une partie de l'espace mémoire d'un serveur physique pour y héberger son application aux côtés d'autres applications stockées sur le même serveur, dans le cadre d'un hébergement mutualisé (*shared hosting*, solution très peu coûteuse).

En plus de ces deux options physiques, le propriétaire a le choix entre deux autres options virtuelles s'il souhaite héberger son application sur un serveur virtuel. Un serveur virtuel est un logiciel programmé sur le serveur physique qui simule à lui seul toute l'activité d'un serveur physique. Ainsi, en stockant plusieurs de ces programmes sur un espace mémoire très étendu, **un même serveur physique peut abriter plusieurs serveurs virtuels**¹⁰⁹⁰. De ce progrès

¹⁰⁹⁰ Ce progrès technique s'inscrit dans l'histoire de la virtualisation informatique. Dès 1962, l'Université de Manchester développe sur son ordinateur Atlas la première mémoire virtuelle, i.e. un programme qui crée un espace mémoire dépassant les capacités de la machine physique à faire circuler

technique est née la première option virtuelle à disposition du propriétaire d'une application. Il peut d'abord réserver la totalité de l'espace mémoire d'un serveur virtuel pour y héberger son application. Cette solution est dite « hébergement privé virtuel », et le serveur virtuel ainsi privatisable est appelé *Virtual Private Server* (VPS). L'hébergement VPS est une sorte d'hébergement dédié virtuel : le propriétaire de l'application peut configurer le serveur virtuel qu'il réserve comme il l'entend en jouant sur ses paramètres de sécurité (les pare-feux, les sauvegardes, le chiffrement SSH, les mises à jour...), d'administration (privilèges de certains utilisateurs ou de certaines requêtes par rapport à d'autres, redémarrage, augmentation de l'espace mémoire virtuel accordé à l'application...) et de disponibilité (mise à l'arrêt du VPS, choix du port d'accès à son serveur et du nom d'hôte de son serveur...) ¹⁰⁹¹.

Enfin, le propriétaire de l'application peut se saisir d'une deuxième option virtuelle, à savoir l'hébergement cloud. Cette technologie consiste à héberger divers tronçons d'une application (*i.e.* divers fichiers ou groupes de fichiers d'une même application) sur plusieurs serveurs virtuels. Contrairement à l'hébergement VPS, l'hébergement cloud est une sorte d'hébergement mutualisé virtuel : chaque application est dispersée sur plusieurs serveurs virtuels, et chaque serveur virtuel héberge les tronçons de plusieurs applications simultanément. Cette mutualisation de l'espace mémoire virtuel démultiplie l'espace mémoire que peut occuper un service en ligne. Une application peut s'étendre sur une infinité de serveurs virtuels sans rendre ces mêmes serveurs indisponibles aux autres applications cherchant à être hébergées en cloud.

les signaux électriques à travers ses circuits électriques (v. KILBURN T., EDWARDS D. B. G., LANIGAN M. J. et SUMNER F. H., « One-Level Storage System », *IRE Transactions on Electronic Computers*, EC-11, 1962, p. 223-235). En détail, sur le fonctionnement de la mémoire virtuelle : on a vu que toute donnée devant être exécutée par la machine doit être préalablement stockée dans la mémoire vive de cette machine. Les données ainsi stockées le sont dans des « cases » de la mémoire vive, chaque case pouvant stocker un octet. Toute case de la mémoire vive possède une adresse (dite « physique ») pour pouvoir être destinataire de l'octet à stocker avant son exécution. L'espace de la mémoire vive est donc limité par le nombre d'adresses attribuables. Or, le nombre d'adresses physiques attribuables dépend du nombre de combinaisons de 0 et de 1 que peuvent transporter les fils électriques dans la machine. Par exemple, si 20 fils électriques sont réservés au transport des adresses physiques, la machine pourra transporter 2^{20} soit 1 048 576 d'adresses physiques différentes. Les cases de la mémoire vive pourront alors stocker simultanément plus d'1 millions d'octets. L'espace mémoire physique sera dès lors limité à 1 Mégaoctet. La virtualisation de la mémoire permet de dépasser ces limites, en superposant des « pages » ou des « segments » logiciels par-dessus les cases physiques, ce qui offre d'étendre immensément l'espace mémoire, bien au-delà des capacités de circulation des signaux électriques dans la machine. V. par exemple le cours préparé par BELOUADHA Fatima-Zahra et EL EULDJ Mohsine, « Architecture des ordinateurs », sur *EMI.ac.ma* (site web de l'École Mohammadia d'ingénieurs à Rabat), 2010-2011. La mémoire virtuelle a engendré l'apparition de la technologie VM (*Virtual Machine*) dans les années 1960 et surtout 1970, qui consiste à simuler l'activité d'une machine au moyen de programmes reproduisant une ou plusieurs fonctions d'une machine physique. Produit dès 1964, le système d'exploitation CP/CMS d'IBM proposait pour la première fois un programme capable de simuler plusieurs machines virtuelles au sein d'une même machine physique pour permettre l'exécution simultanée par l'ordinateur de tâches requises par plusieurs utilisateurs : v. MEYER R. A. et SEAWRIGHT L. H., « A virtual machine time-sharing system », *IBM Syst. J.*, 9, 1970, p. 199-218

¹⁰⁹¹ V. « Quelles sont les étapes pour installer et configurer votre serveur VPS ? », sur *Blog.LWS-hosting.com*, 27 janv. 2021. LWS est un hébergeur web, *i.e.* un entreprise qui loue ses serveurs aux propriétaires de sites web désireux d'héberger leur site sur internet. De même, pour l'hébergeur OVH, v. : « Premier pas avec un serveur VPS », sur *YouTube.com*, vidéo publiée le 29 sept. 2021 par le compte YouTube OVHcloud

Une application en ligne peut ainsi constamment se développer, s'enrichir de nouvelles données sur l'espace mémoire très extensible du cloud.

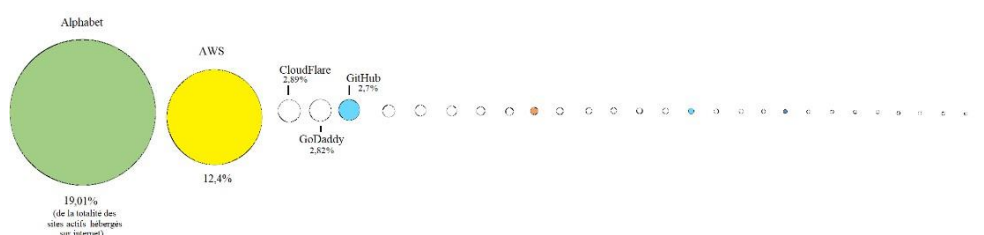
Ce mode d'hébergement fut une petite révolution technique car un serveur cloud peut stocker toutes sortes de données et de fichiers tels : les fichiers de présentation d'une application (éléments graphiques, fonctionnalités à disposition des utilisateurs, contenus d'origine et contenus partagés par les internautes...) ; les fichiers d'accès à une application (noms de domaine, bases de données) ; les fichiers de gestion d'une application (bases de données, gestion des contenus, gestion de la relation client, gestion intégrée, surveillance réseau) et autres algorithmes ; les données relatives aux utilisateurs (collecte de données) ; les fichiers qui recensent les données des utilisateurs collectées et analysées (*cookies*) etc. **À lui seul, un serveur cloud couvre alors des fonctions autrefois remplies par diverses machines** – les serveurs web (pour l'hébergement des fichiers de présentation d'une application), les serveurs de noms de domaines (pour l'hébergement des noms de domaine), les serveurs de base de données (pour l'hébergement de bases de données), les serveurs de collecte (pour l'hébergement des données relatives aux utilisateurs), les serveurs de fichiers (pour l'hébergement de fichiers transférés en ligne par un utilisateur ou une entreprise), les serveurs de messagerie (pour l'hébergement des mails aussi longtemps qu'ils ne sont pas lus par les clients destinataires), les serveurs de gestion d'applications (pour l'hébergement des programmes de gestion des applications), les terminaux ou disques durs externes (pour le stockage par les utilisateurs de la plupart de leurs documents texte, musiques, photos, dessins, images animées, films, séries et autres vidéos). Au lieu d'être éparpillés sur divers types machines, les fichiers d'une application et les données des utilisateurs peuvent tous être hébergés sur des serveurs cloud, faisant du serveur cloud un couteau suisse de l'hébergement de données en ligne. De la même manière que le smartphone recouvre diverses fonctions (réveil matin, appareil photo, agenda, lecteur MP3...), le segment de marché du cloud absorbe une diversité de segments de marché de l'hébergement (marchés de l'hébergement des noms de domaine, de l'hébergement de bases de données, de l'hébergement des données collectées, de l'hébergement de fichiers transférés, de l'hébergement web traditionnel...).

Le cloud a en ce sens un effet très centralisateur sur le fonctionnement de l'hébergement en ligne : toutes les données des utilisateurs et tous les fichiers constitutifs d'une application peuvent désormais être hébergés sur les serveurs cloud d'un même fournisseur d'hébergement, là où ces données et fichiers devaient autrefois être hébergées par divers fournisseurs d'hébergement et/ou par l'utilisateur lui-même (sur son terminal, son disque dur externe etc.). Le chercheur et informaticien Guy Pujolle, qui étudie l'évolution d'internet depuis plusieurs décennies, dresse le même constat d'un réseau internet de plus en plus centralisé par la technologie cloud et par les politiques de routage¹⁰⁹². On en déduit que les serveurs cloud sont des nœuds centralisateurs par leur fonctionnement.

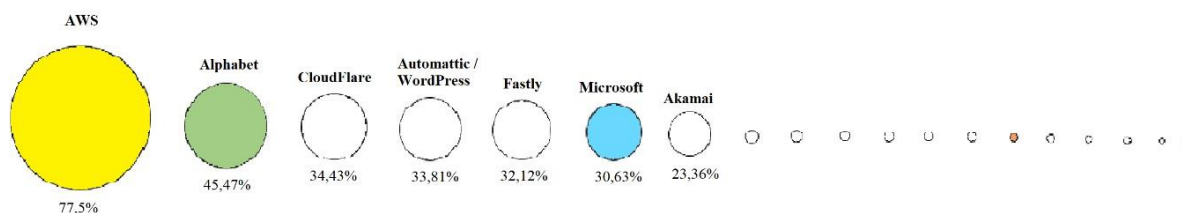
Cette centralisation de l'hébergement suscitée par la technologie cloud a profité une fois encore aux géants, particulièrement à cinq d'entre eux : Alphabet, Amazon et Microsoft, Alibaba et Tencent sur le marché chinois, tous fournisseurs d'hébergement cloud. On a ici classé les différents fournisseurs d'hébergement (cloud ou non) d'après le nombre de sites web qu'hébergent leurs serveurs.

¹⁰⁹² PUJOLLE Guy, *Les réseaux. L'ère des réseaux cloud et de la 5G*, 9^e édition, Eyrolles, 2018

Fournisseurs d'hébergement des 600 866 886 sites web actifs en février 2022



Fournisseurs d'hébergement des 10 000 sites les plus populaires (d'après leur trafic) en février 2022



Alphabet est le premier fournisseur d'hébergement web dans le monde : avec 114 242 239 sites web actifs stockés sur ses serveurs cloud, il **hébergeait 19,01% des 600 866 886 sites web actifs en février 2023**¹⁰⁹³. Deuxième hébergeur mondial, Amazon Web Services (AWS) stockait à la même date 74 529 769 sites web actifs sur ses serveurs cloud, notamment de nombreuses applications en ligne très utilisées mondialement (TikTok, Quora, Netflix, Disney Plus, HBO Max, Fortnite, Onlyfans, SoundCloud, Meesho, Healthline, PhonePe, DMM, ou encore Zillow en plus de ses propres applications IMDb, Amazon, Alexa et Amazon Prime¹⁰⁹⁴). À eux seuls, les trois géants **Alphabet, Amazon et Microsoft** (incluant GitHub) **hébergeaient plus d'un tiers des sites web actifs dans le monde en février 2023**. L'hébergement des applications en ligne est encore plus centralisé du côté des 10 000 sites web les plus visités (d'après leur trafic) : les serveurs d'Amazon concentrent plus de trois quarts des 10 000 sites les plus visités, et ceux d'Alphabet en concentrent plus de 45%. Ce schéma laisse aussi voir combien le cloud a aspiré le marché de l'hébergement : les trois premiers fournisseurs d'hébergement sont des fournisseurs cloud – tandis que GoDaddy fournit de l'hébergement dédié, mutualisé et VPS.

Le cloud a donné aux fournisseurs d'hébergement l'opportunité de spécialiser leurs offres. Basiquement, le fournisseur d'hébergement peut héberger sur ses serveurs cloud des applications pour les mettre à disposition soit des utilisateurs finals, soit des autres propriétaires d'applications. On parle dans ces deux cas de cloud SaaS (*Software as a Service*). Premier type d'applications SaaS : celles destinées aux utilisateurs finals. Toute application hébergée sur des serveurs cloud et destinée à des internautes est une application SaaS (Gmail, Spotify, WeChat, Twitter, Snapchat, Zoom, le jeu vidéo Minecraft... comme la majorité des applications populaires). Deuxième type d'applications SaaS : celles destinées aux propriétaires d'applications. Il s'agit dans ce cas

¹⁰⁹³ « Web Hosting Usage Distribution on the Entire Internet », *Built With* [en ligne, entreprise d'analyse concurrentielle des technologies], consulté le 13 fév. 2023. Pour la part de marché des 10 000 sites web les plus populaires d'après leur trafic, v. « Web Hosting Usage Distribution in the Top 10k Sites », *Built With*, consulté le 13 fév. 2023.

¹⁰⁹⁴ On a recherché en février 2023 sur DNSlytics l'adresse IP du nom de domaine principal de chacune de ces applications, ainsi que l'AS d'appartenance de chacune de ces adresses IP. DNSlytics.com est une base de données qui répertorie les correspondances des noms de domaine et de leurs adresses IP.

de programmes hébergés sur des serveurs cloud dans le but d'aider le propriétaire d'une application à gérer son application.

Par exemple, de nombreux propriétaires d'applications n'ont ni les connaissances pour programmer leur application, ni les moyens d'embaucher un programmeur à cette fin. Le fournisseur d'hébergement cloud peut alors héberger sur ses serveurs un programme de gestion de contenus (WordPress, Wix, Blogger, Dupler, Joomla...) qui met à disposition de ces propriétaires des outils complets et faciles d'utilisation pour créer, structurer et éditer les contenus de leurs applications. À titre d'illustration, si le propriétaire d'une application souhaite créer son site web à l'aide de WordPress, la société Automattic propriétaire de WordPress n'hébergera pas nécessairement les contenus, fonctionnalités et fichiers d'accès au site (noms de domaines et bases de données) ainsi créée. En revanche, elle hébergera une partie des fichiers constitutifs de ce site, à savoir le programme (WordPress) qui pose les fonctions de création, de structuration et d'édition du contenu de ce site. Or, en février 2023, 43,1% des 1,97 milliards de sites web (actifs comme inactifs) dans le monde ont été créés à l'aide de WordPress, soit près de 850 millions de sites web¹⁰⁹⁵. Cela signifie que **si WordPress s'effondre**, 43% des sites web perdent une partie essentielle des fichiers constitutifs de leur existence en ligne – donc **43% des sites web dans le monde s'effondrent avec WordPress**. Shopify est un autre exemple d'application SaaS mise à disposition des propriétaires d'applications. La société Shopify Inc. héberge sur ses serveurs des programmes de gestion de contenus, de relation-client et de gestion intégrée pour proposer aux commerçants les outils de création de leur propre boutique en ligne, de vente et d'achat, de moyens de paiement, de facturation, d'approvisionnement, de comptabilité, de communication avec les acheteurs etc.¹⁰⁹⁶

On a vu que le fournisseur d'hébergement cloud peut héberger des applications sur ses serveurs pour les mettre à disposition sur le réseau. Outre des applications, il peut aussi mettre à disposition des propriétaires d'application un environnement logiciel (système d'exploitation, moteur(s) de bases de données, middleware...) et une infrastructure matérielle d'exécution (serveurs et infrastructures de connexion au réseau, de stockage et de sauvegarde). On parle dans ce cas de cloud PaaS (Platform as a Service). Le propriétaire verra ainsi son application exécutée par les serveurs du fournisseur d'hébergement cloud, en bénéficiant de la qualité d'exécution de l'environnement logiciel et matériel mis à disposition par le fournisseur d'hébergement. L'application sera alors plus fluide d'utilisation pour les internautes tout en épargnant au propriétaire les coûts, l'installation et l'entretien qu'exige l'environnement d'exécution de son application. Outre le SaaS et le PaaS, le fournisseur d'hébergement cloud peut aussi ne mettre que son infrastructure matérielle à disposition du propriétaire d'une application, hors tout environnement logiciel d'exécution. On parle dans ce cas de cloud IaaS (Infrastructure of Service). Plus récemment, certains

¹⁰⁹⁵ « Usage statistics and market share of WordPress », *W3Techs* [en ligne, organisation spécialisée dans l'analyse des technologies web], consulté le 13 fév. 2023

¹⁰⁹⁶ En février 2023, Shopify hébergeait sur ses serveurs cloud 4,6 millions de boutiques en ligne dont 405 parmi les 10 000 sites web les plus visités (v. BuiltWith), ce qui le place devant ses principaux concurrents WooCommerce (un *plugin* de WordPress – i.e. une extension logicielle de WordPress proposée en option – utilisée pour la création de 3,9 millions de boutiques en ligne dont 156 dans le top 10 000), WixStores (4,45 millions de boutiques en ligne dont 50 dans le top 10 000 des sites web), Amplience (6 352 boutiques en ligne dont 183 dans le top des 10 000), Magento (171 162 boutiques en ligne dont 167 dans le top des 10 000 des sites web les plus visités), Squarespace (2,65 millions de boutiques en ligne dont 92 dans le top 10 000) : v. « eCommerce Usage Distribution », sur *builtwith.com*. On estime le nombre d'acheteurs mensuels entre 60 et 80 millions sur Shopify fin 2022.

propriétaires hébergent leur application sur le mode FaaS (*Function as a Service*) : l'application est constamment stockée sur le serveur cloud, mais ce serveur n'alloue à l'application des ressources informatiques que si elle est sollicitée. Cela offre à l'application de consommer un minimum de ressources informatiques, et au propriétaire de payer l'hébergement de son application à proportion des ressources consommées tout en étant débarrassé des questions de configuration, de gestion, de maintenance, de tolérance aux pannes etc.

Malgré la centralisation provoquée par le cloud, plusieurs facteurs sont venus décentraliser le fonctionnement de l'hébergement en ligne. D'abord, les solutions cloud ne sont pas exclusives les unes des autres. Le propriétaire d'une application peut recourir à plusieurs solutions cloud. Par exemple, les applications Zillow (application d'annonces immobilières pour des recherches d'appartements, MAU de 115,5 millions fin 2022), Time Magazine (MAU de 34 millions fin 2022) ou encore les jeux vidéo Angry Birds (MAU de 263 millions fin 2012 mais descendu à 30-45 millions pour l'ensemble des jeux de la gamme fin 2022¹⁰⁹⁷) ont été créées à l'aide de WordPress, ce qui signifie qu'une partie des fichiers constitutifs de ces applications est hébergée sur les serveurs de WordPress (à savoir les fichiers établissant les fonctions de création, de structuration et d'édition des contenus de ces applications). Cependant, les contenus et les noms de domaines de ces trois sites sont hébergés ailleurs – sur les serveurs d'AWS¹⁰⁹⁸. En utilisant plusieurs solutions cloud, ces sites hébergent divers groupes de fichiers par plusieurs fournisseurs d'hébergement.

Ensuite, pour sécuriser l'accès à leur application, de nombreux propriétaires dupliquent sur plusieurs serveurs les fichiers comportant le(s) domaine(s) de leur application. Pour reprendre l'exemple de Time Magazine et d'Angry Birds, ces applications hébergent leurs fonctions de création et d'édition des contenus sur les serveurs de WordPress, leurs contenus et noms de domaines sur les serveurs d'Amazon, mais elles dupliquent par ailleurs leurs noms de domaine sur les serveurs DNS de NS1¹⁰⁹⁹. De même, Discord héberge ses fonctions de messagerie, de création et d'édition des contenus sur les serveurs cloud d'Alphabet mais il héberge ses noms de domaines sur deux serveurs différents de CloudFlare¹¹⁰⁰. De cette façon, si tombe un serveur hébergeant discord.com, l'autre serveur prendra le relai pour transmettre les requêtes DNS et assurer l'accès à l'application Discord. Ou encore, les applications Fandom (wiki tenu par les fans) et Pinterest (réseau social de partage d'images et vidéos) hébergent leurs fonctions de création et d'édition des contenus sur les serveurs d'Amazon, mais leurs noms de domaines sur 4 serveurs DNS d'Oracle (pour Fandom) et 8 serveurs DNS de Fastly (pour Pinterest)¹¹⁰¹. La pratique de duplication des noms de domaines sur une diversité de serveurs – relevant souvent d'autres

¹⁰⁹⁷ GROSS Andy, « What Angry Birds Can Teach Enterprises About Critical Data », *Wired*, fév. 2014 ; Rovio Entertainment Corporation, *Q3 22. Interim Report for January-September 2022*, sur *investors.rovio.com*, 28 oct. 2022, et Rovio Entertainment Corporation, *Full Year and Q4 2022*, sur *investors.rovio.com*, 9 fév. 2023

¹⁰⁹⁸ Les domaines zillow.com, time.com et angrybirds.com portent respectivement les adresses IP publiques 52.84.93.24, 52.222.158.19 et 3.137.114.90 (d'après la base de données myip.ms). Or, ces trois adresses IP sont membres de l'AS16509 d'Amazon (d'après la base de données dnslytics.com). Autrement dit, ces trois adresses IP correspondent aux routeurs passerelles d'Amazon qui connectent à internet les serveurs hébergeant zillow.com, time.com et angrybirds.com.

¹⁰⁹⁹ Entrées « angrybirds.com » et « time.com » sur la base de données myip.ms (pour obtenir leurs différentes adresses IP), et recherche de leurs adresses IP sur dnslytics.com/reverse-ip (pour obtenir leur AS d'appartenance)

¹¹⁰⁰ Même opération qu'à la note de bas de page précédente avec l'entrée « discord.com »

¹¹⁰¹ Même opération qu'à la note de bas de page précédente avec les entrées « fandom.com » et « pinterest.com » sur les bases de données myip.ms et dnslytics.com/reverse-ip

fournisseurs d'hébergement que ceux hébergeant les fonctions de messagerie, de création et d'édition des contenus – permet de décentraliser le fonctionnement de l'hébergement en ligne, donc de sécuriser l'hébergement des applications. La décentralisation apportée par cette pratique doit néanmoins être largement relativisée dans les faits : les diverses copies d'un domaine sont le plus souvent hébergées par un même fournisseur d'hébergement, voire par un même système autonome (AS).

Enfin, une autre pratique s'est développée ces dix dernières années : la copie sur des serveurs cloud, non des domaines, mais des contenus de l'application (ceux soumis aux utilisateurs par le propriétaire de l'application et ceux partagés par les utilisateurs). Certains fournisseurs d'hébergement proposent aux propriétaires d'applications d'héberger leurs fichiers de contenus en les dupliquant sur une multitude de serveurs éparpillés dans le monde (par exemple en France, au Brésil, au Japon...) ¹¹⁰². Cette option permet non seulement d'alléger la charge d'un seul serveur hébergeant les contenus, mais aussi de stocker le contenu à des emplacements stratégiques en le rapprochant géographiquement des internautes (français, brésiliens, japonais...). Ce réseau de serveurs qui héberge les copies des contenus est appelé « réseau de diffusion de contenus » (ou CDN pour *Content Delivery Network*). En rapprochant les contenus des internautes, le CDN réduit la longueur des routes pour accéder aux contenus de l'application, donc limite le risque de perte de données en cours de route et accélère l'accès aux contenus par l'internaute. Par exemple, on a vu que Fandom héberge ses fonctions de création et d'édition de contenus sur les serveurs d'Amazon, et qu'elle héberge les duplications de ses noms de domaine sur les serveurs d'Oracle ; mais elle héberge ses contenus sur un CDN fourni par Fastly et constitué de 101 adresses IP éparpillées dans le monde.

De même, le réseau social Pinterest héberge ses fonctions de création et d'édition de contenus sur les serveurs d'Amazon, duplique ses noms de domaine sur les serveurs de Fastly, mais héberge ses contenus sur des CDN fournis par Akamai (1719 adresses IP), Fastly (55 adresses IP), Amazon (29 adresses IP) et CloudFlare (5). Plus encore, cette application utilise l'application SaaS de messagerie fournie par les serveurs cloud d'Alphabet, et elle utilise l'application SaaS fournie par Adobe Ads pour diffuser des publicités sur sa plateforme ¹¹⁰³. **In fine, les fichiers constitutifs de l'application Pinterest s'étendent sur au moins 2 030 adresses IP** (1808 adresses IP pour le CDN, 202 pour le réseau de serveurs publicitaires d'Adobe Ads, 8 pour les noms de domaine, 5 pour la messagerie, et 11 pour les fonctions de création, d'édition et de partage de contenus, les bases de données, le middleware, les algorithmes de traitement...) **réparties entre six fournisseurs d'hébergement** (Amazon, Fastly, Alphabet, Akamai, CloudFlare et Adobe). Quant au forum Reddit, son hébergement s'étend sur au moins 261 adresses IP (133 pour le CDN fourni par Fastly, 4 pour les duplications de noms de domaines hébergées par Amazon, 5 pour l'utilisation d'une application de messagerie SaaS fournie par

¹¹⁰² Précisément, les contenus sont dupliqués sur des serveurs de cache. Un serveur de cache est un serveur qui héberge des fichiers le temps d'une requête seulement (stockage bref). Par exemple, l'internaute qui souhaite accéder à l'application Facebook adresse sa requête à destination du serveur de cache de Facebook le plus proche ; lorsque le serveur de cache reçoit la requête, il demande au serveur hébergeant l'application Facebook de lui transmettre uniquement les fichiers requis par l'utilisateur ; une fois les fichiers réceptionnés par le serveur de cache, ce dernier peut les communiquer à l'utilisateur. De cette façon, la requête de l'utilisateur n'est pas obligée d'atteindre le serveur éloigné qui héberge Facebook, mais peut obtenir le résultat de sa requête en accédant au serveur de cache le plus proche. Les serveurs de cache sont aussi souvent utilisés pour héberger des publicités, et sont également employés par les FAI pour accélérer l'acheminement des requêtes.

¹¹⁰³ Profil de Pinterest sur la base de données Netify.ai, entreprise spécialisée dans l'analyse des réseaux numériques des entreprises

Alphabet, 7 pour l'utilisation de l'application SaaS de diffusion de publicités fournie par Branch IO, 1 pour l'utilisation de l'application SaaS fournie par Atlassian de suivi et de gestion des incidents, de gestion des tâches et d'un espace de travail en équipe, et 111 pour l'hébergement par Amazon des contenus, des fonctions de création, de partage et d'édition des contenus, des bases de données, du middleware...) réparties entre cinq fournisseurs d'hébergement (Amazon, Fastly, Alphabet, Branch IO, Atlassian)¹¹⁰⁴.

A priori, les CDN contribuent à décentraliser l'hébergement d'une application, mais cette décentralisation doit être là encore très relativisée, voire se révèle comme un faux-semblant. En effet, tous les serveurs hébergeant des contenus n'assurent pas exactement la même fonction. Lorsque le propriétaire de l'application ne déploie aucun CDN, il héberge classiquement ses contenus sur au moins un serveur (d'Amazon par exemple), et les internautes ne pourront accéder à ces contenus qu'en accédant à ce serveur. En revanche, lorsque le propriétaire de l'application déploie un CDN (fourni par Fastly par exemple), ses contenus sont toujours hébergés sur le serveur d'origine fourni par Amazon ; les serveurs fournis par Fastly se contentent de relayer au serveur d'origine les requêtes d'accès aux contenus. Par conséquent, seul le serveur d'origine assure la fonction d'hébergement permanent des contenus. Les serveurs membres du CDN (appelés serveurs edge) assurent une fonction de relai et dépendent tous du ou des serveurs d'origine hébergeant le contenu. Si le serveur d'origine tombe, les serveurs edge ne pourront plus relayer les requêtes jusqu'au serveur d'origine, donc ne pourront plus permettre l'accès aux contenus. Dès lors, le recours à un CDN ne sécurise pas davantage l'hébergement des contenus : que le propriétaire de l'application se serve ou non d'un CDN, l'effondrement du même nœud (serveur d'origine) produit les mêmes conséquences (inaccessibilité des contenus) dans les deux scénarii. Sous cet éclairage, les CDN ne décentralisent guère le fonctionnement de l'hébergement en ligne, et contribuent même à centraliser les connexions de serveurs – une multitude de nœuds émetteurs ou destinataires (serveurs Edge) est connectée par un serveur d'origine dont elle dépend. Loin de décentraliser l'hébergement du contenu, **les CDN ressemblent à des instruments d'expansion des applications qui procèdent d'une centralisation : de la connexion des serveurs** (nombre de serveurs Edge connectés par un même serveur d'origine) ; **et du fonctionnement de l'hébergement en ligne** (dépendance des serveurs Edge au serveur d'origine).

En somme, début 2023, les éléments de décentralisation apportés par le cloud (possibilité pour le propriétaire de l'application de recourir à diverses applications SaaS, PaaS et IaaS) sont moindres par rapport à la centralisation de l'hébergement en ligne provoquée par le cloud (absorption d'une grande diversité de segments de marchés par le segment du cloud, concentration par les serveurs cloud de l'hébergement de tout type de données y compris les contenus, données personnelles des utilisateurs et duplications de noms de domaine, concentration de l'hébergement des applications en ligne par Alphabet, Amazon et Microsoft, dépendance croissante des sites web à certaines applications SaaS comme WordPress, Adobe, Shopify, large domination des segments PaaS, IaaS et du cloud privé par Amazon, Microsoft et Alphabet¹¹⁰⁵, dépendance croissante de réseaux de serveurs à un même serveur d'origine hébergeant les contenus...).

¹¹⁰⁴ Profil de Reddit sur la base de données Netify.ai

¹¹⁰⁵ Le cloud privé consiste à héberger les données d'une entreprise auxquelles seule cette entreprise peut accéder, contrairement aux données hébergées en cloud public qui sont accessibles à tous, et aux données hébergées en cloud hybride qui ne sont accessibles qu'à certains et/ou sous certaines conditions (« What is a private cloud ? Private cloud vs. Public cloud » sur cloudflare.com). Au troisième trimestre 2022, les revenus d'AWS sur les segments de marché du PaaS, de l'IaaS et du cloud privé représentaient 34% de l'ensemble des revenus générés mondialement par ces marchés, les revenus de Microsoft Azure en représentaient 21%, et ceux d'Alphabet en représentaient 11%. Au total, les trois géants concentraient donc 66% des revenus, en hausse de 5 points (61%) par rapport au

Chapitre 2. Évaluation de l'efficacité de l'action régulatrice sur internet

L'étude de la centralisation nous a permis d'évaluer les effets de cette technique de restriction sur la gestion d'internet, sur son fonctionnement et sur les connexions qu'il suscite. Pour autant, aussi efficace ait été cette technique pour (re)définir la structure du réseau, est-elle efficace pour contrôler l'échelle de diffusion des données dans le cyberspace ?

On observera que tel n'est pas le cas : les réseaux les plus centralisés (Chine, Russie, Corée du Nord) connaissent des contournements massifs de la part des prescripteurs numériques pour accéder à des R-DATA, souvent même plus massifs que dans des réseaux moins centralisés. Il en va de même pour les applications : le fait qu'une application soit centrale est bien loin de garantir le contrôle des données hébergées par cette application, et a même tendance à faciliter la diffusion de R-DATA à grande échelle. Inversement, les techniques de régulation par augmentation de l'accès ont fait plusieurs fois leurs preuves pour réduire l'échelle de diffusion d'une donnée - à condition, dans la plupart des cas, d'être accompagnées des techniques de restrictions adaptées.

Ce dernier Chapitre passera en revue sept techniques d'augmentation de l'accès, puis expérimentera les conditions de leur efficacité (Section 1). Enfin, on analysera les différentes configurations de contournement possibles sur internet, et on proposera une théorie et des solutions pour contrôler efficacement l'échelle de régulation d'une donnée dans le cyberspace d'après la méthode de la régulation (Section 2).

Section 1. Techniques de régulation par augmentation de l'accès

On divise les techniques d'augmentation en deux catégories : les techniques qui augmentent incidemment l'accès à des A-DATA, parce qu'elles facilitent l'accessibilité des A-DATA autant que celle des R-DATA (Paragraphe 1) ; et les techniques qui augmentent spécialement l'accès à des A-DATA, à l'exclusion des R-DATA. Pour cette dernière catégorie, on distinguera les techniques selon qu'elles sont basées sur le trafic (Paragraphe 2) ou sur les services et contenus stockés en ligne (Paragraphe 3).

Paragraphe 1 – Techniques pour augmenter incidemment l'accès à des A-DATA

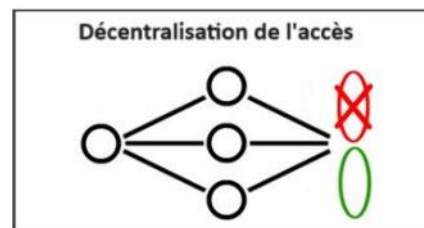
Parmi ces techniques d'augmentation « incidente », seront successivement abordés la décentralisation (A), le raccordement (B) et l'accélération non-discriminée de l'accès (C).

A) La décentralisation de l'accès à internet

On a vu que la régulation peut consister à restreindre l'accès à une R-DATA (donnée refusée par le régulateur) dans le but de réduire l'échelle de diffusion de cette R-DATA. Elle peut aussi consister à augmenter l'accès à une A-DATA (donnée admise par le régulateur) de façon à faire croître l'échelle de diffusion de cette A-DATA. Il s'agit dans ce cas de promouvoir certaines données que le régulateur espère voir plus largement diffusées, et non plus de limiter certaines données que le régulateur espère voir moins largement diffusées. On étudie ici plusieurs techniques d'augmentation de l'accès praticables dès la transmission de données, à commencer par la décentralisation de l'accès à internet.

troisième trimestre 2021, de 7 points (59%) par rapport au troisième trimestre 2020 et de 8 points (58%) par rapport au troisième trimestre 2019 : Synergy Research Group, « Q3 Cloud Spending Up Over \$11 Billion from 2021 Despite Major Headwinds; Google Increases its Market Share », sur [srgresearch.com](https://www.srgresearch.com), 2022.

On appelle « décentralisation » la technique qui consiste à diversifier les voies d'accès à une même donnée empruntables par un nœud émetteur. Elle correspond à la configuration inverse à celle de la centralisation (restriction de la diversité des voies d'accès à une donnée).



On reconnaît plusieurs avantages et inconvénients à la décentralisation. Premier avantage : **la décentralisation**

renforce la viabilité d'un réseau numérique, i.e. sécurise ce réseau contre une large diffusion d'un problème technique, d'une erreur humaine, d'une catastrophe naturelle et d'une cyberattaque. Tandis que la centralisation généralise les failles d'un nœud auprès d'un grand nombre de nœuds qui en dépendent, la décentralisation sectorise les failles auprès du groupe réduit de nœuds qui en dépendent.

Cela implique d'une part que, en décentralisant le fonctionnement, la conception et la connexion du réseau, cette technique réduit non seulement le nombre de personnes dépendantes d'un nœud central mais aussi le risque que l'effondrement du nœud central provoque celui de la fonction exclusivement assurée par ce nœud. Par exemple, si un seul terminal assure la fonction de coordination des installations d'un complexe nucléaire, une cyberattaque menée contre ce terminal peut faire s'effondrer la mise en œuvre de cette fonction et engendrer une paralysie voire une extinction d'un site nucléaire entier ; si un seul câble sous-marin assure la fonction de transport des données par voie sous-marine, la dégradation voire la destruction de ce câble par un séisme, une éruption volcanique ou un tsunami peut faire s'effondrer toute la fonction de transport sous-marin des données ; si un seul système d'exploitation est utilisé par tous les terminaux travaillant sur un projet militaire, les failles de ce système d'exploitation peuvent être utilisées par un cyberattaquant pour corrompre tous les terminaux travaillant sur ce projet (dépendance d'un grand nombre de nœuds à un logiciel de conception central – ici un système d'exploitation) ; si un seul réseau de serveurs cloud héberge tous les fichiers des applications en ligne les plus utilisées, ces applications et leurs utilisateurs s'exposent à un risque élevé de panne générale affectant simultanément toutes ces applications, d'un vol massif de données personnelles hébergées sur le même serveur ou encore d'une large diffusion d'un logiciel malveillant (dépendance d'un grand nombre de nœuds connectés à un réseau de serveurs central)... *A contrario*, la viabilité du réseau est renforcée si plusieurs nœuds assurent la même fonction, si un nombre minimal d'utilisateurs dépend d'un même nœud et si les matériels, logiciels et langage de conception sont variés pour accéder à internet. D'une part, donc, la décentralisation a pour double effet de limiter la survenance des menaces qu'on vient de voir (en sécurisant le fonctionnement du réseau) et d'en réduire l'échelle de diffusion (en diminuant le nombre de nœuds dépendants d'un nœud susceptible de pannes, d'erreurs de gestion ou d'attaques).

D'autre part, la sectorisation des nœuds issue de la décentralisation implique une décongestion du réseau. En effet, si un seul routeur assume l'acheminement d'un très grand nombre de données, ce routeur central est fortement exposé à un risque de congestion, i.e. de saturation des capacités d'exécution du routeur face à la quantité de trafic à traiter. De même, si un seul serveur assume l'exécution d'un très grand nombre de requêtes et le stockage d'un très grand nombre de données, ce serveur central est lui aussi fortement exposé au risque de congestion. Inversement, si la gestion du trafic et du stockage de données est également réparti entre divers routeurs et serveurs, le même volume de données peut être partagé entre plusieurs nœuds. Pour un même volume de données, la décentralisation permet donc à chaque routeur et

à chaque serveur d'assumer une quantité de données moindre comparativement à celle supportée par un nœud central. En limitant la survenance d'une congestion, la décentralisation favorise ainsi la réduction du risque de saturation, l'accélération du trafic ou encore la diminution du risque de déperdition de données.

Deuxième avantage : en plus de renforcer la viabilité du réseau, **la décentralisation diminue les conséquences sociales, économiques, administratives et politiques des pannes et des attaques mais aussi des erreurs, décisions et actions des gestionnaires centraux**. Par exemple, la centralisation fait peser sur le nœud central la responsabilité économique de l'innovation, car l'innovation ne progresse pas sous l'effet d'une égale concurrence entre plusieurs sources de propositions économiques (*i.e.* plusieurs offrants) mais sous l'effet d'une source monopolistique qui n'a pas droit à l'erreur pour faire croître l'innovation. De même, si les gestionnaires centraux sont des acteurs privés, leurs décisions et actions politiques peuvent affecter des centaines de millions voire milliards de personnes, imposant ainsi à travers le réseau numérique des politiques à plus de la majorité d'une population nationale et concurrençant potentiellement les politiques étatiques. Il en va ainsi de Google Search, dont la censure des contenus (non-référencés sur le moteur) et les critères de cette censure s'appliquent à plus de 3,6 milliards de personnes chaque mois. Inversement, la décentralisation implique une diversité des fabricants de terminaux, des gestionnaires de réseaux de transport, d'acheminement et de serveurs, mais aussi une réduction de l'audience des applications en ligne très utilisées. En somme, dans un réseau décentralisé et par rapport à un réseau centralisé, non seulement les pannes, erreurs et attaques ont moins de risque de survenir et de se diffuser, mais aussi les décisions politiques des acteurs privés ont moins de champ pour s'étendre socialement, la responsabilité de l'économie ne dépend pas des décisions et erreurs d'un gestionnaire central, les administrations importantes ne menacent pas de s'effondrer sous l'effet d'une attaque...

En revanche, on voit deux inconvénients de taille à la décentralisation. Premier inconvénient : on a vu que **la décentralisation rend plus difficile une généralisation des mesures de régulation auprès d'un grand nombre de nœuds**. La régulation d'un réseau décentralisé ne peut donc reposer que sur un respect des règles par un très grand nombre d'acteurs. Cela implique, d'une part, que la décentralisation fait reposer l'efficacité des mesures de régulation sur une large coopération des acteurs concernés. Or, un devoir de coopération trop large aggrave le risque d'inefficacité desdites mesures. En effet, plus il y a d'acteurs nécessaires à l'application générale d'une règle, plus il y a de risque que l'application de la règle soit biaisée voire empêchée par les différentes interprétations faites de cette règle, par les difficultés à l'appliquer et par les refus de l'appliquer. D'autre part, l'impossibilité de généraliser des mesures de régulation implique une excellente interopérabilité (entre les protocoles utilisés, les nombreuses applications utilisées, les logiciels locaux et différents systèmes d'exploitation...). En d'autres termes, les exigences d'interopérabilité augmentent à mesure que le réseau se décentralise.

Deuxième inconvénient : **la décentralisation facilite le contournement des techniques de restriction**. En effet, la décentralisation diversifie les voies d'accès à une donnée, et fournit donc à l'utilisateur de multiples moyens pour accéder à un nœud en contournant les nœuds qui pratiquent la restriction. Concrètement, si l'utilisateur peut accéder à vingt opérateurs, mais que seuls quinze d'entre eux appliquent scrupuleusement le blocage d'un site web, cet utilisateur peut accéder à ce site web en empruntant le réseau d'un des cinq opérateurs ne pratiquant pas le blocage. De même, si de nombreuses applications concurrentes sont facilement accessibles

aux utilisateurs, ces derniers peuvent migrer depuis une application restrictive vers une application concurrente plus permissive. En facilitant le contournement, la décentralisation aggrave ainsi le risque d'inefficacité des mesures de restriction.

Dans l'Union Européenne, l'accès à internet a d'abord été régulé par la technique de la décentralisation. En effet, durant les années 1990, les Communautés européennes faisaient de la libéralisation de la fourniture de l'accès la priorité en matière d'accès à internet¹¹⁰⁶. En 1987, la Commission européenne accepte le maintien des droits exclusifs ou spéciaux pour désigner une entreprise monopolisant la fourniture de réseaux de télécommunications (par ex. France Telecom) ou pour limiter le nombre d'opérateurs qui fournissent ces réseaux, mais appelle les États à faire respecter la libre concurrence sur tous les autres services de télécommunication¹¹⁰⁷. Il faudra attendre 1990 pour qu'une directive exige aux États membres d' « *assurer (...) l'abolition des droits exclusifs ou spéciaux pour la fourniture de services de télécommunications autres que le service de téléphonie vocale et prennent les mesures nécessaires afin de garantir le droit de tout opérateur économique de fournir lesdits services de télécommunications* »¹¹⁰⁸. Cette directive est révisée en 1996 pour définir une date – le 1^{er} janvier 1998 – à laquelle les États doivent abolir ces droits exclusifs ou spéciaux et permettre à toute personne de fournir des services de télécommunications ou d'exploiter des réseaux de télécommunication¹¹⁰⁹.

Toutefois, l'abolition des droits exclusifs ou spéciaux n'a pas fait disparaître un obstacle important pour l'ouverture du marché : jusque dans les années 1990, les ex-monopoles (France Telecom en France, duopole de BT et Mercury au Royaume-Uni...) étaient les seuls à avoir pu déployer sur le territoire leurs câbles, antennes-relais et autres infrastructures de transport des communications électroniques – principalement les communications téléphoniques à l'époque. Malgré la libéralisation européenne, les ex-monopoles concentraient donc toujours la très grande majorité des installations nécessaires à la fourniture d'accès, et les opérateurs concurrents n'étaient alors pas en mesure de déployer un réseau rivalisant avec celui des ex-monopoles. En nous exprimant avec les termes de la théorie concurrentielle, on peut dire que les ex-monopoles concentraient les « facilités essentielles » sur le marché de la fourniture d'accès, i.e. les outils et moyens « *indispensables à l'exercice d'une activité économique (...) [pour lesquels] il n'existe ni substitut réel ni substitut potentiel* »¹¹¹⁰. Afin de réduire l'accaparement des facilités essentielles par un petit nombre d'opérateurs voire un opérateur unique, l'Union européenne engage en 2000 une politique dite de « dégroupage ». Le

¹¹⁰⁶ CURIEN Nicolas, « La libéralisation des télécommunications en Europe », *Flux*, n° 44-45, 2001, p. 28-35

¹¹⁰⁷ Commission européenne, Livre vert sur le développement du marché commun des services et équipements de télécommunications, 30 juin 1987, COM/87/290 final

¹¹⁰⁸ Directive 90/388/CEE de la Commission du 28 juin 1990 relative à la concurrence dans les marchés des services de télécommunication, art. 2

¹¹⁰⁹ Directive 96/19/CE du 13 mars 1996 modifiant la directive 90/388/CEE en ce qui concerne la réalisation de la pleine concurrence sur le marché des télécommunications, art. 1^{er}, 2) : « *les États abolissent toutes les mesures accordant : (a) des droits exclusifs pour la fourniture de services de télécommunications et l'exploitation de réseaux de télécommunications (...); ou (b) des droits spéciaux qui limitent à deux ou plus (...) le nombre d'entreprises autorisées à fournir ces services de télécommunications ou à exploiter ces réseaux* »

¹¹¹⁰ DEZOBRY Guillaume, *La théorie des facilités essentielles*, LGDJ, Bibliothèque de droit international et communautaire, p. 33

dégrouper consiste à imposer aux ex-monopoles de mettre à disposition des opérateurs concurrents les ressources concentrées par ces ex-monopoles (câbles et infrastructures réseau, fréquences hertziennes attribuées, informations sur l'emplacement des points d'accès physiques, modalités technique d'accès et d'utilisation de ces ressources...) nécessaires pour fournir aux utilisateurs finals un accès à un vaste réseau de communications électroniques. Un règlement communautaire de 2000 oblige ainsi les opérateurs en position très dominante à dégrouper l'accès à leur réseau, soit totalement (l'opérateur soumis à l'obligation de dégrouper transfère la propriété de ses fréquences et infrastructures) soit en accès partagé (l'opérateur soumis à l'obligation de dégrouper met à disposition ses fréquences et infrastructures dont il reste propriétaire)¹¹¹¹. Ce faisant, l'UE a privilégié la décentralisation du transport et de l'acheminement en obligeant les États membres à diversifier les voies d'accès à internet et leurs gestionnaires privés.

En 2002, l'UE s'efforce d'accroître la décentralisation de l'acheminement et du transport en émettant quatre directives (appelées « premier paquet télécom »). La directive-cadre homogénéise l'action et la coopération des Autorités Réglementaires Nationales de télécommunication (ARN, comme l'Arcep en France, l'Ofcom au Royaume-Uni...) en leur fixant trois missions communes : promouvoir la concurrence dans la fourniture de réseaux de communications électroniques (en veillant à une concurrence non entravée ni faussée, en encourageant des investissements et en soutenant l'innovation, en encourageant l'utilisation et la gestion efficace des radiofréquences...) ; contribuer au développement du marché intérieur (en supprimant les derniers obstacles à la fourniture de réseaux de communications électroniques, en encourageant le développement de réseaux transeuropéens et l'interopérabilité des services paneuropéens, en veillant à l'absence de discrimination dans le traitement des opérateurs...) ; et soutenir les intérêts des citoyens de l'UE (en assurant à tous les citoyens un accès minimal aux services de communication électronique, en encourageant la fourniture d'informations claires comme la transparence des tarifs et des conditions d'utilisation des services de transmission de données, en garantissant l'intégrité et la sécurité des réseaux de communications publics, en répondant aux besoins d'accès des handicapés...)¹¹¹². La libre concurrence doit ainsi être assurée à long terme par lesdites autorités. Toujours dans le sens d'une décentralisation du réseau européen, la même directive requiert des États membres qu'ils encouragent l'utilisation de normes techniques internationales pour garantir l'interopérabilité des services de fourniture d'accès dans l'UE, invite ces États à favoriser le partage des câbles et équipements entre opérateurs pour éviter aux nouveaux entrants sur le marché d'obtenir les autorisations nécessaires à l'utilisation voire à l'expropriation du bien foncier occupé par ces câbles et équipements, et assigne aux ARN la mission d'identifier les « entreprises puissantes » parmi les opérateurs de transmission de données (i.e. les entreprises qui sont « en mesure de se comporter (...) de manière indépendante de ses concurrents, de ses clients et (...) de consommateurs »)¹¹¹³.

Les trois autres directives détaillent les grandes orientations de la directive-cadre. La directive « autorisations » instaure un régime de notification (dit d'autorisation générale) pour toute personne désireuse de fournir un réseau de communications électroniques – permettant à cette personne de fournir son réseau en se contentant de notifier l'existence de son service à l'ARN sans nécessiter de décision expresse de l'ARN ni autre acte administratif de sa part –, et un régime d'autorisation individuelle pour les entreprises qui exploitent les fréquences hertziennes

¹¹¹¹ Règlement (CE) n° 2887/2000 du Parlement européen et du Conseil du 18 décembre 2000 relatif au dégrouper de l'accès à la boucle locale, art. 2, 3 et Annexe

¹¹¹² Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, art. 8

¹¹¹³ *Ibid.*, art. 17, 12 et 14

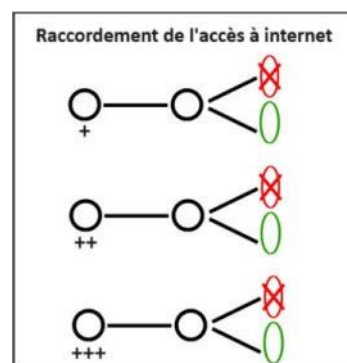
et pour les entreprises puissantes – assurant ainsi une utilisation et une répartition efficaces des fréquences hertziennes et permettant aux ARN d’assortir d’obligations spécifiques les autorisations accordées à ces entreprises ¹¹¹⁴. La directive « accès » pose la pleine liberté contractuelle des opérateurs pour conclure des accords de peering (interconnexion entre les réseaux de deux opérateurs différents) et des contrats favorisant l’accès des opérateurs aux ressources grâce auxquelles ils peuvent exercer à leur activité (accès aux logiciels pertinents, aux pylônes, gaines et bâtiments, aux câbles et lignes détenus par les ex-monopoles comme France Telecom, contrats d’itinérance...) ¹¹¹⁵. Elle interdit aux États membres d’entraver cette liberté contractuelle, à l’exception des entreprises puissantes que la directive soumet à cinq obligations spécifiques : obligations de transparence (publication d’un offre de référence par l’opérateur puissant), de non-discrimination (vis-à-vis des opérateurs qui souhaitent accéder au réseau des opérateurs puissants ou s’y interconnecter), de séparation comptable (pour éviter toute discrimination ou obtention de subventions croisées abusives), de fourniture de ressources spécifiques (pour assurer l’interopérabilité entre les différents réseaux), et de respect des décisions de l’ARN sur un éventuel contrôle des prix. Enfin, on examinera la directive « service universel » un peu plus loin. Les directives « autorisations » et « accès » persistent à ouvrir le marché de la fourniture d’accès à internet, en assouplissant le régime d’autorisation et en renforçant l’indépendance contractuelle et d’interconnexion des fournisseurs d’accès.

En somme, la décentralisation qu’on a observée pour les réseaux d’acheminement britanniques et français s’inscrivent le cadre d’une législation européenne poussant fortement à la décentralisation. *A contrario*, on a vu qu’en Chine, la législation nationale a orienté la structure du réseau vers une configuration très centralisée. Enfin, en Russie, on a vu que la législation fédérale a d’abord promu une forte décentralisation des réseaux d’acheminement et de transport dans la deuxième moitié des années 1990 par la libéralisation du marché, avant de favoriser une structure réseau fortement centralisée depuis 2019.

B) Le raccordement de l’accès à internet

1. Les politiques de raccordement au Royaume-Uni

On appelle « raccordement » la technique qui consiste à connecter un nœud émetteur et un nœud destinataire dans le réseau internet. Concrètement, le raccordement consiste à fournir un accès internet à un nœud émetteur, ou à étendre son accès à de nouveaux nœuds destinataires. Cette technique d’augmentation correspond à la configuration inverse à celle de la coupure de l’accès examinée plus haut (technique de restriction).



Comme les autres méthodes de régulation examinées, le raccordement possède ses avantages et inconvénients. Premier avantage : le raccordement à internet permet de **maintenir les liens sociaux, professionnels et économiques entre les êtres humains indépendamment de l’état de leurs contacts physiques**. De cette façon, le

¹¹¹⁴ Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l’autorisation de réseaux et de services de communications électroniques, cons. 17 et art. 3 et 5

¹¹¹⁵ Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l’accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu’à leur interconnexion, art. 2, 3 et 12

raccordement offre la possibilité : aux entreprises de mener leurs activités à distance (contacts en ligne avec les fournisseurs, travailleurs libéraux et autres partenaires, réduction des coûts de location, des charges, de la maintenance et des équipements pour l'employeur qui recourt au télétravail, réduction des frais de déplacement, de parking ou de déjeuner des employés qui pratiquent le télétravail...) ; aux administrations d'accroître leurs relations avec les administrés (applications en ligne administratives comme vie-publique.fr, legifrance.fr, la plateforme France Connect...) ; et aux organismes, de façon générale, d'accélérer le traitement des demandes (applications justice.fr et Télérecours pour saisir le juge, passage d'une commande auprès d'un prestataire de services, demande d'assistance à une association...). De même, le raccordement fait pleinement ses preuves durant les crises qui entravent voire empêchent les déplacements individuels – guerres, pandémies, catastrophes climatiques... En somme, le raccordement à internet consolide l'organisation d'une société face aux problèmes posés par (temps de déplacement) et à (restrictions de déplacement) la circulation physique des êtres humains.

Deuxième avantage : **le raccordement à internet permet de faire germer une nouvelle source d'économie** – l'économie numérique. Cela signifie que, du côté des utilisateurs, il favorise leur accès à de nouveaux services. Du côté des commerçants (fabricants et vendeurs de terminaux, opérateurs, publicitaires, fournisseurs de systèmes d'exploitation et d'applications en ligne, influenceurs...), le raccordement augmente leur clientèle (acheteurs, abonnés, nombre de personnes exposées à des publicités, audience et donc attractivité et clientèle publicitaires...) et leurs profits. Sur le plan de la théorie économique, ces nouveaux biens, services, dépenses et profits participent à l'augmentation de la production de biens et de services, donc favorisent la croissance économique – hausse de la valeur totale de la production de richesse.

On voit en revanche deux inconvénients au raccordement. Premier inconvénient : **le raccordement peut rendre les relations sociales, administratives, professionnelles et économiques dépendantes d'internet** si les utilisateurs (civils comme professionnels), administrations et commerçants s'y reposent excessivement. Une telle dépendance implique en effet que ces divers segments de la société obéissent de plus en plus aux lois d'internet telles qu'on les a identifiées (lois de la neutralité et de l'interopérabilité exécutives, loi de la solidarité applicative, et lois d'interconnexion binaire, protocolaire et opérationnelle) : les cyberattaquants peuvent prescrire l'exécution d'un logiciel malveillant par les machines de milliers d'entreprises, d'institutions publiques, d'établissements de santé, de sites et industries essentielles (transports en commun, gestion et distribution de l'eau et de l'électricité...) ou dominantes dans une économie nationale (PSA, Renault, Total, Vivendi) ; les utilisateurs peuvent prescrire l'exécution par leur terminal de leur requête destinée à faire stocker par des serveurs un contenu haineux ou une fausse information, de façon à faire acquérir à ces contenus nocifs une échelle de diffusion auprès de millions voire centaines de millions d'autres utilisateurs ; les organisations les plus centrales dans un réseau internet national (fabricants de terminaux comme Microsoft ou Samsung, opérateurs comme Orange, fournisseurs de systèmes d'exploitation comme Apple, propriétaires d'applications en ligne comme Alphabet ou Meta...) peuvent prescrire et donc imposer leurs politiques aux machines de dizaines de millions voire de milliards d'utilisateurs à échelle mondiale. Le raccordement d'une société humaine à internet aggrave donc le risque que cette société soit exposée à une amplification de l'échelle de diffusion des comportements néfastes et à une soumission croissante des populations à des politiques privées. Deuxième inconvénient : **le raccordement ne permet pas de cibler spécifiquement l'accès à une A-DATA**, donc ne permet pas de favoriser davantage l'accès aux A-DATA qu'aux R-DATA. Certes, contrairement aux techniques de restriction examinées, le raccordement permet d'augmenter le nombre de personnes qui peuvent accéder à une A-DATA grâce à internet, mais il augmente tout autant le nombre de personnes qui peuvent accéder à une R-DATA. En ce sens, le raccordement est une technique de régulation qui n'offre

pas la possibilité d'augmenter exclusivement le nombre de personnes susceptibles d'accéder à une A-DATA, mais offre au mieux la possibilité d'augmenter incidemment ce nombre.

On s'intéresse ici au raccordement prescrit par le droit de l'UE. On a vu que, dans les années 1990-début 2000, l'UE a d'abord régulé l'accès à internet par la libéralisation et l'ouverture du marché de la fourniture d'accès (décentralisation dès la transmission de données). Depuis 2002, le droit de l'UE régule aussi l'accès à internet par l'extension de la fourniture d'accès au plus grand nombre possible d'abonnés¹¹¹⁶. La technique ici mobilisée ne relève plus de la décentralisation, mais du raccordement afin de connecter toute la population européenne à internet. Partie intégrante du premier paquet télécom, la directive « services universels » de 2002 exige aux États membres de « *veiller à ce que les services [universels] soient mis à la disposition de tous les utilisateurs finals sur leur territoire, indépendamment de leur position géographique, au niveau de qualité spécifié [dans la directive] et, compte tenu des circonstances nationales particulières, à un prix abordable* »¹¹¹⁷. Les six services universels énumérés par la directive sont : (i) la mise à disposition du public de postes téléphoniques moyennant paiement pour leur utilisation (cabines téléphoniques) ; (ii) la fourniture d'un réseau téléphonique au public ; (iii) la mise à disposition du public d'un service lui permettant de donner et recevoir des appels nationaux et internationaux et d'accéder aux services d'urgence ; (iv) l'établissement d'un plan national de numérotation géographique (indicatifs téléphoniques, par ex. 33 pour la France, 01 pour les numéros de téléphone fixe situés en Île-de-France, 02 pour ceux situés en Région Nord-Ouest...) ; (v) l'établissement d'un plan national de numérotation non géographique (définition d'un plan d'attribution des numéros autres que les indicatifs géographiques, par ex. en France 06 ou 07 pour les numéros de mobile, 0800 à 0805 pour les numéros d'appel gratuits, 081, 082, 089 suivis de 4 chiffres pour les numéros majorés ou surtaxés...) ; (vi) et enfin la fourniture à un abonné d'un service d'accès à un « *réseau de communications public* », y compris les réseaux « *utilisant l'acheminement* »¹¹¹⁸.

Le Royaume-Uni n'a pas attendu les directives européennes pour libéraliser puis étendre la fourniture d'accès à des services de communications électroniques. En 1981, le *Telecommunications Bill* donne naissance à l'opérateur public BT, alors en situation de monopole. En 1982, le gouvernement britannique autorise l'opérateur privé Mercury, filiale de Cable & Wireless, à exploiter des fréquences hertziennes et à fournir à des abonnés un réseau de transmission des communications électroniques. En 1984, BT est privatisée et l'ancêtre de

¹¹¹⁶ Certes, un plan d'action de déc. 1984 émis par le Conseil européen énonce pour grands objectifs la « *création d'un marché communautaire des terminaux et équipements de télécommunications* », le « *développement de services et de réseaux avancés de télécommunication* » et l'« *amélioration de l'accès des régions défavorisées de la Communauté aux avantages du développement de services et de réseaux avancés* » – trois objectifs qui vont dans le sens d'une extension de la fourniture d'accès à un plus grand nombre d'utilisateurs. Cependant, ces objectifs ne s'accompagnent d'aucune obligation ni sanction, ni même de mesures très précises mais seulement d'une homogénéisation des normes techniques tirées de normes internationales, d'une reconnaissance mutuelle des agréments des terminaux, d'une mise en discussion des projets d'infrastructure d'intérêt commun et d'un projet de développement des technologies nécessaires à l'établissement de réseaux futurs à haut débit, d'un appel à faire une « *utilisation appropriée des instruments financiers communautaires* », et de la mise en place d'un réseau par vidéocommunication pour les responsables politiques de la Communauté. Le plan d'action est exposé dans la Revue du marché commun, n° 284, fév. 1985, p. 120 [en ligne]

¹¹¹⁷ Directive 2002/22 du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, art. 3

¹¹¹⁸ *Ibid.*, art. 2

l'Ofcom, l'OfTel (*Office of Telecommunications*), est créée pour veiller au respect de la libre concurrence sur le marché. Pour éliminer progressivement le monopole de BT, le Royaume-Uni ouvre progressivement les marchés des terminaux en 1982, de la téléphonie mobile en 1985, des infrastructures locales depuis 1987 et des cabines téléphoniques en 1988 – entamant ainsi le processus de libéralisation 5 ans avant l'appel du Livre vert européen de 1987. En 1992, le ministère britannique du commerce et de l'industrie libéralise totalement le marché de la fourniture d'accès à des réseaux de communications électroniques – soit deux ans après la directive européenne réclamant l'abolition des droits exclusifs et spéciaux sur ce marché et six ans avant la date butoir européenne pour réaliser cette libéralisation¹¹¹⁹.

Le Royaume-Uni a ainsi été le premier pays européen à décentraliser son réseau de transmission des données par l'ouverture, la libéralisation et la privatisation du marché de la transmission des communications électroniques. Il fut aussi parmi les premiers pays européens – si ce n'est le premier – à généraliser le raccordement pour étendre l'accès à son réseau de transmission par la population nationale. Dès les années 1990, l'OfTel délivre les autorisations d'exploitation de fréquences hertziennes à condition que les titulaires des autorisations couvrent une partie du territoire britannique ; puis en juillet 1995, dans le cadre d'un document intitulé « *Effective Competition – a framework for action* », l'OfTel définit sept ans avant l'UE les obligations de service universel comme « *la fourniture sur l'ensemble du territoire d'un service téléphonique vocal et de services associés (facturation détaillée, sélection des appels, aide aux handicapés) à un prix raisonnable (« geographic accessibility, affordable access, equitable access »)* »¹¹²⁰.

En 2003, le Royaume-Uni ratifie la directive services universels dans le cadre du *Communications Act*. Cette loi attribue de nouvelles missions et compétences à l'Ofcom, notamment les missions « *d'assurer l'utilisation optimale du spectre électromagnétique par la télégraphie sans fil (...) et la disponibilité dans tout le Royaume-Uni d'un large éventail de services radio* »¹¹²¹. Surtout, le *Communications Act* charge l'Ofcom de désigner les personnes tenues de fournir les services universels listés par la directive. La même année, le Secrétaire d'État britannique au commerce et à l'industrie édicte le décret sur le service universel (*Universal Service Order*). Cet décret détaille, pour chacun des services universels listés par la directive européenne, les obligations des personnes désignées par l'Ofcom, et oblige au moins l'une de ces personnes à « *répondre à toutes les demandes raisonnables des utilisateurs finals concernant le raccordement (...) au réseau téléphonique public* » et à « *donner aux utilisateurs finals la capacité d'effectuer et de recevoir (...) des communications de données, à des débits suffisants pour permettre un accès fonctionnel à Internet* »¹¹²². L'Ofcom désigne les opérateurs BT et Kingstone Communication (devenu KCOM) pour fournir les services universels, dont

¹¹¹⁹ Sur toutes les informations de ce paragraphe, v. THONIER Axel, « Dix ans de réforme des télécommunications au Royaume-Uni : échec du pilotage de la structure de marché et libéralisation complète », *Économie & prévision*, 1995, p. 107-125

¹¹²⁰ *Ibid.*, p. 117

¹¹²¹ Ofcom, « Coverage and planning policy for analogue radio broadcasting services », 2 mars 2005

¹¹²² Par ex., obligation pour les personnes désignées de mettre à disposition des utilisateurs finaux au moins un annuaire sous une forme électronique, de fournir aux clients les informations sur les modes de facturation, les modes d'acceptation des paiements et les avantages tarifaires pour l'utilisation des services de communications électroniques etc. V. Minister of State for Energy, E-Commerce and Postal Services, Department of Trade and Industry, *The Electronic Communications (Universal Service) Order*, 2003

l'accès minimal à internet, et réalise en 2005 sa première évaluation du respect de leurs obligations par BT et KCOM¹¹²³. Depuis, l'Ofcom a progressivement élargi les obligations de couverture du territoire (en y ajoutant les obligations pour tout opérateur exploitant des fréquences hertziennes de couvrir certain pourcentage de la population, de la surface territoriale et de locaux résidentiels, professionnels, administratifs...) et a rehaussé le débit minimal devant être minimalement fourni par BT et KCOM (passant d'une obligation de fournir un bas-débit inférieur à 56 Kbit/s à une obligation de fournir un haut-débit d'au moins 10 Mbit/s en 2015)¹¹²⁴.

2. Les politiques de raccordement en France

La France a suivi la même trajectoire, plus tardivement. En France, la régulation, la décentralisation et le raccordement de la transmission de données interviennent à des dates très rapprochées par rapport au Royaume-Uni. Concernant la régulation de la transmission de données, l'Oftel britannique (devenu l'Ofcom) a vu le jour en 1984 tandis que l'ART française (devenue l'Arcep) est instituée treize ans plus tard en janvier 1997. Concernant la décentralisation du réseau de transmission, la France attend la date-butoir fixée par la directive européenne – le 1^{er} janvier 1998 – pour libéraliser le marché de la fourniture d'accès à internet en abolissant les droits exclusifs accordés à France Telecom¹¹²⁵, soit six ans après le Royaume-Uni. France Telecom est privatisée en 2004¹¹²⁶, soit vingt ans après la privatisation de BT.

Concernant le raccordement, la loi de 1996 qui organise la libéralisation du marché prévoit du même coup les obligations de service universel, un an après la définition par l'Oftel du service universel téléphonique. Cette loi fixe trois principaux objectifs pour la « *régulation du secteur des télécommunications* » : la liberté d'activité dans le domaine des communications électroniques (autrefois appelées télécommunications) ; l'indépendance de la régulation du secteur vis-à-vis de l'exploitation et de la fourniture des services de communications électroniques ; et « *le maintien et le développement du service public des télécommunications [France Telecom], qui comprend notamment le droit de chacun au bénéfice du service universel des télécommunications* »¹¹²⁷. À cette fin, poursuit le texte, le ministre chargé des

¹¹²³ Ofcom, « Universal Service Obligation », 10 janvier 2005-21 mars 2005

¹¹²⁴ Concernant les obligations de couverture du territoire, les titulaires d'une autorisation d'exploitation des fréquences doivent ainsi, depuis 2012, être « capables de fournir des services de télécommunications mobiles dans une zone où vit au moins 90 % de la population du Royaume-Uni » (contre 80% dans les autorisations antérieures à 2012), et « avec une probabilité de 90 % que les utilisateurs situés à l'extérieur de cette zone puissent recevoir le service avec un débit d'au moins 768 Kbits/s » : Ofcom, « 3G Coverage Obligation Verification Methodology », 9 mai 2012. En 2018, dans le but d'améliorer la connexion internet dans les ruralités, l'Ofcom semble axer ses exigences sur le pourcentage de la surface géographique couverte (90% de l'Angleterre, 90% de l'Irlande du Nord, 74% de l'Écosse et 83% du Pays de Galle fin 2018), le nombre de locaux connectés à internet et le nombre de sites d'infrastructures réseau déployés par les opérateurs mobile : Ofcom, « Coverage obligations in the 700 MHz and 3.6-3.8 GHz spectrum award. Ofcom's approach to verifying compliance », 31 janv. 2019. Concernant le passage d'une obligation de bas-débit à une obligation de haut-débit pour le service universel, v. Ofcom, « Designing the broadband universal service obligation », avr. 2016

¹¹²⁵ Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications, art. 22, II

¹¹²⁶ Loi n° 2003-1365 du 31 décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom, art. 7

¹¹²⁷ Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications, art. 2

télécommunications et l'ART « *veillent (...) à la prise en compte de l'intérêt des territoires et des utilisateurs dans l'accès aux services et aux équipements* ».

Pour accélérer la couverture numérique du territoire, le législateur de 2001 donne aux collectivités locales le pouvoir de mettre leurs infrastructures « *destinées à supporter des réseaux de télécommunications* » à disposition des opérateurs (infrastructures dites passives comme les pylônes, gaines, bâtiments, points haut...), tout en interdisant à ces mêmes collectivités locales la possibilité d'exercer elles-mêmes les activités d'opérateur¹¹²⁸. En 2003, la France transpose la directive service universel de 2002, au même moment que le Royaume-Uni. La loi de transposition désigne France Telecom en qualité d'opérateur responsable de garantir les services universels en France, et l'oblige ainsi à « *assurer l'acheminement des communications téléphoniques, des communications par télécopie et des communications de données à des débits suffisants pour permettre l'accès à Internet, en provenance ou à destination des points d'abonnement, ainsi que l'acheminement gratuit des appels d'urgence* »¹¹²⁹.

Dès le début des années 2000 – peut-être même dès la fin des années 1990 – on trouve des traces d'une obligation de couverture réseau dans les autorisations délivrées par l'Autorité de régulation des télécommunications (ART, ancêtre de l'Arcep)¹¹³⁰. En effet, l'ART conditionnait la délivrance d'autorisations d'exploitation des fréquences par l'obligation, pour le titulaire de l'autorisation, de respecter un « cahier des charges » fixé par l'ART et qui incluait des objectifs de couverture réseau du territoire¹¹³¹. L'ART reconnaissait toutefois une certaine limite aux obligations de déploiement qu'elle peut imposer à des opérateurs privés : en certains endroits du territoire, une couverture de qualité n'est pas rentable pour les opérateurs privés dont l'objectif est la recherche d'un profit, voire n'est pas viable économiquement pour eux¹¹³². Cette limite constitue le principal obstacle au déploiement du réseau sur le territoire. Les zones qui ne sont couvertes par aucun opérateur sont appelées « zones blanches ». Pour éliminer les zones blanches, l'ART appelle le législateur à faire germer des opérateurs locaux en supprimant l'interdiction faite aux collectivités locales d'exercer les activités d'opérateur, et en assouplissant le régime d'autorisation qui conditionne la fourniture d'un réseau de communications électroniques.

En 2004, le législateur applique les recommandations de l'ART et transpose la directive « autorisations » : les autorisations de l'Arcep ne sont désormais requises que pour les demandes d'exploitation des fréquences hertziennes, et ne le sont plus pour le déploiement d'un

¹¹²⁸ Loi n° 2001-624 du 17 juillet 2001 portant diverses dispositions d'ordre social, éducatif et culturel, art. 19 (V), modifiant l'art. L511-6 du code général des collectivités territoriales

¹¹²⁹ Loi n° 2003-1365 du 31 décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom, art. 1^{er}

¹¹³⁰ Autorité de régulation des télécommunications, « Réponse de l'Autorité de régulation des télécommunications à la consultation publique relative à l'évolution du droit français des communications électroniques » [en ligne sur *Arcep.fr*], 2002

¹¹³¹ Par exemple, en 2003, le point 1-3 du cahier des charges de SFR obligeait cet opérateur à couvrir 99% de la population d'ici 2011 : Conseil de la concurrence, Avis n° 2002-A-04 du 11 avril 2002 relatif à l'acquisition par la société Télédiffusion de France d'un ensemble de sites pylônes de la société Bouygues Telecom

¹¹³² Autorité de régulation des télécommunications, « Réponse de l'Autorité de régulation des télécommunications à la consultation publique relative à l'évolution du droit français des communications électroniques » [en ligne sur *Arcep.fr*], 2002, p. 58s.

réseau numérique par un opérateur ; et les collectivités locales gagnent la compétence d'exercer les activités d'opérateur¹¹³³. Afin de couvrir les zones blanches, la LCEN de 2004 privilégie deux techniques supplémentaires proposées par le premier paquet télécom européen de 2002 : l'itinérance ; et la mutualisation de réseaux. La première technique, l'itinérance, permet à l'abonné qui se situe dans une zone non couverte par son opérateur d'emprunter le réseau d'un opérateur tiers qui couvre cette zone. Par exemple, si Mayotte est couverte par les infrastructures d'Orange mais n'est pas couverte par celles de Bouygues Telecom, les abonnés de Bouygues Telecom peuvent emprunter le réseau d'Orange pour passer et recevoir des appels téléphoniques ou pour se connecter à internet. L'itinérance est généralement permise par l'interconnexion des réseaux des opérateurs, l'échange entre opérateurs de données authentifiantes (carte SIM, nom d'utilisateur/pseudo...) et de facturation des abonnés dans le cadre d'accords d'itinérance. Dans ce cas, l'opérateur O1 accueille sur son réseau les abonnés de l'opérateur O2, mais seules les fréquences de O1 sont exploitées. La deuxième technique, la mutualisation des réseaux, consiste pour un opérateur O1 à partager ses infrastructures avec un opérateur O2 de façon que les fréquences des deux opérateurs sont exploitées¹¹³⁴. La LCEN oblige ainsi les opérateurs à communiquer au gouvernement et à l'Arcep « *un projet de répartition des zones* » par points d'itinérance et par points de mutualisation de réseaux ainsi qu'un « *projet de calendrier prévisionnel de déploiement des pylônes et d'installation des équipements électroniques de radiocommunication* ». D'après le délai fixé par la loi, les opérateurs ont trois ans (jusqu'en juin 2007) pour achever l'ensemble du déploiement.

En somme, tant en France qu'au Royaume-Uni, le raccordement a été principalement réalisé à travers les obligations de couverture numérique, l'assouplissement des procédures administratives et des interdictions légaux afin de faciliter la fourniture d'un réseau de communications électroniques à des abonnés, et le partage des infrastructures (itinérance et mutualisation des réseaux)¹¹³⁵. Le Royaume-Uni a toutefois largement devancé la France concernant la régulation des communications électroniques, la décentralisation et le raccordement du réseau de communications électroniques. La tardiveté de la régulation française explique probablement le retard de la France dans l'évolution du nombre de personnes connectées à internet : entre 2000 et 2004, la part des ménages français ayant accès à internet passe de 12% à 30-32%, tandis que la part des ménages britanniques ayant accès à internet passe de 27% à plus de 50% sur la même période¹¹³⁶. Le retard français dans le déploiement du réseau, conjugué avec une culture française plus interventionniste que celle britannique, expliquent aussi probablement une autre différence entre les régulations française et britannique : pour accélérer

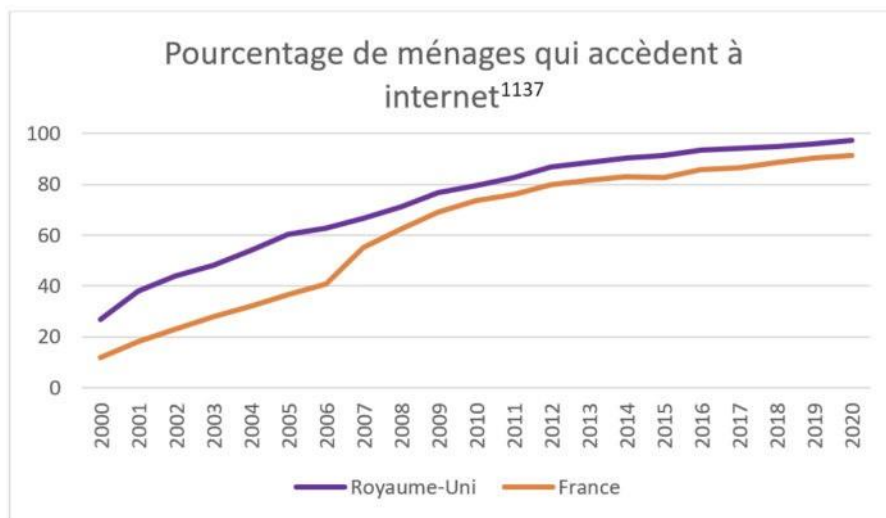
¹¹³³ Respectivement : loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, art. 22, II ; et loi pour la confiance numérique (LCEN) de 2004, art. 50

¹¹³⁴ Arcep, « Le partage de réseaux mobiles », mis à jour le 8 déc. 2022

¹¹³⁵ Dès les années 1990, l'Ofcom délivrait les autorisations d'exploitation de fréquence en y insérant une condition d'itinérance nationale : Ofcom, « National roaming », 16 sept. 2003

¹¹³⁶ V. respectivement : OCDE, « Accès des ménages à l'ordinateur et à l'internet » in *Panorama des statistiques de l'OCDE 2005* [en ligne], 2005, p. 129 ; OCDE, « Taux d'accès Internet » [en ligne], mis à jour en 2022 ; BELOT Claude, « Haut débit et territoires : enjeu de couverture, enjeu de concurrence », Rapport d'information n° 443 du Sénat, 29 juin 2005, p. 32

la couverture du territoire et le raccordement durant les années 2000, la France a démultiplié les fonds public-privé comme on le détaillera *infra*.



C) L'accélération non-discriminée de l'accès à internet

Depuis la deuxième moitié des années 2010, la très grande majorité des populations européennes utilise internet. Les inégalités numériques d'une population (« *fracture numérique* », « *digital divide* »...) résident alors moins dans la capacité d'accéder à internet que dans la qualité de l'accès et dans les compétences d'utilisation d'internet. Les inégalités de compétence numérique renvoient à la notion d'illectronisme, i.e. le « *manque de compétences numériques de base* »¹¹³⁸. L'Insee identifie quatre domaines de compétences numériques de base : la recherche d'information ; la communication ; la résolution de problèmes ; et l'usage de logiciels¹¹³⁹. Dans les faits, le manque de maîtrise de ces compétences se traduit par exemple par l'incapacité à faire des virements en ligne, à demander des crédits bancaires, à suivre les transferts d'argent, à rédiger un CV, à postuler un emploi, à réserver une place dans un train ou un avion, à demander une aide associative, ou encore à suivre les procédures administratives dématérialisées (paiement des impôts en ligne, dépôt de plainte en ligne, demande d'aides publiques, suivi de son compte Pôle Emploi...)¹¹⁴⁰. En 2019, l'Insee évaluait ainsi à 41% la part de personnes âgées de 60 ans ou plus en situation d'illectronisme dans la région Grand Est, contre 3% la même année et dans la même région pour les moins de 30 ans¹¹⁴¹. Quant aux inégalités dans la qualité

¹¹³⁷ OCDE, « Accès des ménages à l'ordinateur et à l'internet » in *Panorama des statistiques de l'OCDE 2005* [en ligne], 2005, p. 129 ; OCDE, « Taux d'accès Internet » [en ligne], mis à jour en 2022

¹¹³⁸ Insee, « Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base », *Insee Analyses Grand Est*, n° 154, 20 déc. 2022

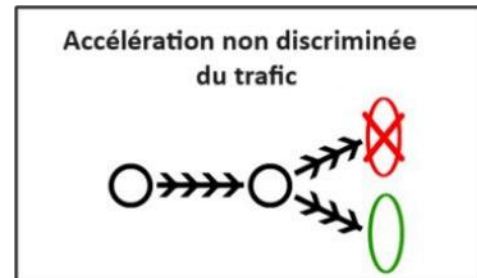
¹¹³⁹ *Ibid.*

¹¹⁴⁰ KESTEMAN Nadia, « Entre illettrisme et illectronisme. Les nouveaux publics à faible autonomie administrative », *Revue des politiques sociales et familiales*, n° 135, 2020, p. 65-73 ; PONTIER Jean-Marie, « Lutte contre l'illectronisme ? », *AJDA*, 2020, p. 2225-2228 ; HE Linxin, « La sécurité sociale à l'ère du numérique : quel renouveau de la solidarité ? », *Revue de droit sanitaire et social (RDSS Dalloz)*, p. 301-318

¹¹⁴¹ Insee, « Une personne sur six... », préc., 2022

d'accès, elles renvoient surtout aux différences de vitesse de trafic entre les utilisateurs, voire aux différences de sécurisation et d'intégrité des données des utilisateurs. De nombreux États européens tentent aujourd'hui de lutter contre ces deux types d'inégalités numériques – qualité de l'accès et compétences d'utilisation. On se focalisera ici sur les différences de vitesse d'accès entre utilisateurs (qualité de l'accès).

Pour réduire les inégalités dans la qualité d'accès à internet, de nombreux États coordonnent ou promeuvent un vaste déploiement des technologies accélérant la vitesse de trafic (4G, 5G, fibre optique...). On appelle « accélération non-discriminée de l'accès à internet » la technique de régulation qui consiste à augmenter la vitesse du trafic internet pour toute requête, ce qui permet de réduire les temps de latence pour mener des activités à distance.



On voit deux principaux avantages à cette technique. D'une part, **l'accélération non-discriminée du trafic favorise le développement économique des entreprises**. En effet, cette technique amplifie les flux d'information, de biens et de capitaux provenant d'une entreprise, *i.e.* la quantité d'échanges économiques entre une entreprise, ses salariés, ses partenaires et ses clients. Par exemple, la rapidité avec laquelle un utilisateur peut accéder à une application, y publier ou y consulter des messages, puis passer à une autre application facilite et accroît la consommation des applications en ligne par les utilisateurs. D'autre part, **l'accélération non-discriminée du trafic améliore la coordination des différents segments de la société connectés à internet**. Le progrès scientifique est stimulé par la rapidité de communication et la quantité de messages échangés entre chercheurs, l'action publique peut plus efficacement et promptement synchroniser les administrations, la prise en charge médicale d'urgence peut être accrue... L'accélération non-discriminée du trafic maximise les avantages du raccordement. Inversement, **l'accélération non-discriminée du trafic aggrave** aussi les inconvénients du raccordement, et principalement **le risque de dépendance de la société humaine au réseau internet**. Le deuxième inconvénient que l'on reconnaît à cette technique tient à **l'impossibilité de favoriser les A-DATA plus que les R-DATA**. L'accélération non-discriminée améliore autant l'accès aux A-DATA que l'accès à la R-DATA. Comme les techniques d'augmentation précédemment étudiées, cette technique ne peut donc contribuer qu'incidemment à l'augmentation de l'échelle de diffusion d'une ou plusieurs A-DATA. Enfin, on relève un troisième inconvénient commun avec le raccordement : **l'accélération du trafic aggrave le risque d'inégalités d'accès**, notamment dans la comparaison entre zones intensément/peu couvertes, entre foyers équipés/non-équipés des dernières technologies (3G, 4G, 5G...), entre foyers aisés/pauvres etc.

Au Royaume-Uni comme en France, l'Ofcom et l'Arcep ont très activement mené des politiques de couverture du territoire en haut débit puis en très haut débit. L'Union Internationale des Télécommunications définit **l'accès internet à haut débit** comme une vitesse de trafic d'au moins 256 Kbit/s¹¹⁴². Cette vitesse correspond notamment aux

¹¹⁴² « Définitions des statistiques internationales – Connexions Internet haut débit » (Begriffserläuterungen zur Internationalen Statistik – Breitband-Internetanschlüsse), Destatis [Office fédéral allemand de la statistique] sur Web.archive.org, 2012

technologies **ADSL** (exploitation des lignes de cuivre en réservant au transport de données la partie du spectre hertzien non utilisée par le transport de la voix) et à la plupart des technologies **3G** (technologie de téléphonie mobile permettant le transport simultané de la voix et des données, sachant que la vitesse de la 3G rurale est de seulement 144 Kbit/s contre 384 Kbit/s pour la 3G urbaine et 1900 Kbits/s soit 1,9 Mbit/s pour la 3G fixe, pouvant atteindre 42 Mbit/s avec la 3.75G). Quant à l'**accès internet à très haut débit**, il est défini en Europe à partir d'une vitesse de 30 Mbit/s (contre 25 Mbit/s aux États-Unis)¹¹⁴³. Cette vitesse correspond notamment à la **fibres optique** (de 300 Mbit/s à 8000 Mb/s soit 8 Gb/s) et à la plupart des technologies **4G** (de 10 Mbit/s à 3 Gbit/s). Enfin, la technologie 5G en cours de déploiement propose une vitesse du trafic variant de 5 Gbit/s à 70 Gbit/s.

En France, le déploiement du haut-débit a principalement eu lieu dans le cadre des « cycles d'analyse de marché ». Ces cycles sont des programmes proposées par l'Arcep, d'une durée de trois ans en général, à l'occasion desquels l'Arcep impose des obligations particulières aux opérateurs puissants¹¹⁴⁴. Lors des cycles 2005-2008 puis 2008-2011, l'Arcep a ainsi étendu les obligations de ces opérateurs en matière de couverture haut-débit¹¹⁴⁵. Dès les débuts du déploiement haut débit, l'ART s'est attachée à baisser les tarifs d'accès aux offres ADSL, en décembre 2003 puis en février 2005¹¹⁴⁶. En plus des obligations de couverture et de la régulation des prix, l'Arcep a promu l'utilisation de certaines technologies pour améliorer l'accès haut débit entre 2005 et 2009 – comme l'emploi généralisé sur le territoire de la technologie READSL2 capables de fournir l'ADSL à longue distance du central téléphonique (pour étendre l'accès haut débit aux personnes éloignées du central), ou encore le raccourcissement des paires de cuivre (pour accélérer l'ADSL)¹¹⁴⁷. Parallèlement à la régulation par l'Arcep, le gouvernement et le législateur français ont multiplié les fonds d'investissement publics-privés afin d'accélérer la couverture haut débit en France entre 2001 et 2009¹¹⁴⁸.

¹¹⁴³ Arcep, Observatoire des marchés des communications électroniques, « Services fixes haut et très haut débit (marché de détail) », 28 fév. 2013, p. 3 : « Afin de se conformer aux seuils fixés par la Commission Européenne dans le cadre de son agenda pour l'Europe à l'horizon 2020, l'ARCEP adopte la définition du seuil du très haut débit de la Commission qui est de 30 Mbit/s ». Aux États-Unis, la FCC envisage de monter le seuil « très haut débit » au seuil minimal de 100 Mbit/s : VELAZCO Chris, « FCC calls 25 Mbps 'broadband' speed. The push is on to up it to 100 », *The Washington Post*, 19 juil. 2022

¹¹⁴⁴ Arcep, Conférence du presse du 8 avril 2011, sur *Arcep.fr*

¹¹⁴⁵ Arcep, « L'accès haut débit via l'ADSL », sur *Arcep.fr*, mis à jour en juin 2018

¹¹⁴⁶ *Ibid.*

¹¹⁴⁷ ART, Avis du Comité d'Experts du 17 mai 2005 concernant l'autorisation de la technique READSL2 au répartiteur dans le cadre de l'accès à la boucle locale de France Télécom ; Arcep, « Mise en œuvre de l'accès à la sous-boucle et articulation avec le développement du très haut débit », oct. 2009

¹¹⁴⁸ Le 9 juillet 2001, le gouvernement engage un plan d'action avec l'objectif de couvrir la totalité du territoire en téléphonie mobile d'ici 2004, et met en place un « dispositif de soutien public à l'investissement des collectivités territoriales afin de généraliser l'accès à internet à haut débit en France » (Autorité de régulation des télécommunications, « Adapter la régulation au nouveau contexte du marché des télécommunications », Rapport, juil. 2002, p. 59). Le 15 juillet 2003, l'État signe une « convention nationale » avec les opérateurs et associations d'élus dans le but de mettre en œuvre un « plan d'extension de la couverture du territoire en téléphonie mobile ». Dans le cadre de ce programme destiné à couvrir les zones blanches, les collectivités territoriales sont invitées à mettre à disposition des opérateurs des « infrastructures passives (pylônes, points hauts...) que ces derniers s'engagent à équiper des infrastructures de transmission nécessaires » (Circulaire

Quant à la couverture très haut débit, le gouvernement définit en 2013 un programme national de déploiement de la fibre optique appelé « Plan France Très Haut Débit » (PFTHD). Promis par le candidat François Hollande durant la campagne présidentielle de 2012, le PFTHD est juridiquement acté le 29 avril 2013 par un arrêté du premier ministre qui renvoie à un cahier des charges de 48 pages posant les objectifs, les étapes et le cadre du déploiement¹¹⁴⁹. Le Plan prévoit l'objectif de couvrir 80% des logements par fibre optique d'ici 2022, et d'y consacrer 20 milliards € en investissements publics-privés. À ces fins, le territoire est divisé en deux types de zones. Les zones d'initiative privée comprennent 57% de la population française, et désignent les communes dans lesquelles le déploiement de fibre est rentable pour les opérateurs privés. Dans ces zones, les opérateurs sont obligés de couvrir la population en fibre optique, et doivent investir 6-7 milliards € dans cette perspective. Les zones d'initiative publique comprennent 43% de la population française, et désignent les communes dans lesquelles le déploiement de fibre n'est pas rentable pour les opérateurs privés. Dans ces zones, ce sont les collectivités locales qui sont obligées de couvrir la population en 4G et en fibre optique, et doivent à ce titre investir les 13-14 milliards € restants. Pour mener cette mission, les collectivités locales peuvent être subventionnées par à l'État à hauteur de 7 milliards sous conditions (réalisation d'un réseau en fibre optique par la collectivité, inscription du projet dans un cadre au moins départemental, objectifs de couverture d'au moins 80% sur leur territoire...), de sorte que l'État prendrait en charge au moins la moitié des investissements publics locaux.

Parallèlement et en soutien aux initiatives gouvernementales, l'Arcep veille à l'extension du très haut débit en France. Dès 2007-2008, l'Arcep impose à France Telecom de mettre ses infrastructures de génie civil (fourreaux et supports aériens) à disposition des opérateurs alternatifs pour leur donner les moyens de déployer de la fibre optique¹¹⁵⁰. Les obligations de France Telecom pour assurer l'accès à ses infrastructures de génie civil sont si étendues que l'Autorité de la concurrence demande de les alléger dans les territoires à forte animation concurrentielle¹¹⁵¹. Durant la décennie 2010, l'Arcep met en œuvre un véritable programme de déploiement de la fibre optique. Pour ce faire, elle distingue les Zones Très Denses (ZTD,

NOR/LBL/B/04/10062/C du 28 juillet 2004, « Fonds de compensation pour la TVA », p. 6). Le 17 décembre 2009 est promulgué la loi relative à la lutte contre la fracture numérique, qui crée un « *fonds d'aménagement numérique des territoires* » pour soutenir le déploiement des infrastructures réseau pour l'accès au haut débit « à un coût raisonnable » dans les zones où l'Arcep estime que les opérateurs ne sont pas en mesure de fournir un tel accès (Loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique).

¹¹⁴⁹ Arrêté du 29 avril 2013 relatif à l'approbation du cahier des charges de l'appel à projets « France très haut débit - Réseaux d'initiative publique » ; Cahier des charges de l'appel à projets « France Très Haut Débit - Réseaux d'initiative publique », 2013, disponible sur « Le plan France Très Haut Débit », *Arcep.fr*, maj le 12 juin 2023

¹¹⁵⁰ Arcep, Avis n° 2007-0745 du 20 septembre 2007 relatif à la demande d'avis du Conseil de la concurrence portant sur la demande de mesures conservatoires déposée par la société Free relative à des pratiques de la société France Télécom sur le secteur des infrastructures de génie civil dans le secteur des communications électroniques ; Arcep, Décision n° 2008-0835 du 24 juillet 2008 portant sur la définition du marché pertinent de gros des offres d'accès aux infrastructures physiques constitutives de la boucle locale filaire, sur la désignation d'un opérateur exerçant une influence significative sur ce marché et sur les obligations imposées à cet opérateur sur ce marché

¹¹⁵¹ Autorité française de la concurrence, Décision n° 08-D-02 du 12 février 2008 relative à une demande de mesures conservatoires présentée par la Free SAS et concernant l'accès aux infrastructures de génie civil de France Télécom dans le cadre du déploiement de boucles locales optiques résidentielles de type FTTh

communes à forte concentration de population sur le territoire desquelles le déploiement de la fibre est économiquement viable pour les opérateurs) des Zones Moins Denses (ZMD, toutes les autres communes)¹¹⁵². Cette distinction permet à l'Arcep d'imposer aux opérateurs des obligations assez exigeantes pour le déploiement de fibre dans les ZTD, et des obligations de couverture plus progressives dans les ZMD¹¹⁵³. Un nouveau coup d'accélérateur est donné en 2018 : alors que se renouvelaient les autorisations des quatre principaux opérateurs, l'Arcep conditionne ce renouvellement par un ensemble d'obligations constitutives du programme « New Deal Mobile »¹¹⁵⁴. Ce programme, destiné à généraliser la 4G, se poursuit avec l'établissement par l'Arcep d'un calendrier que les quatre principaux opérateurs doivent respecter entre 2019 et 2030. Ce calendrier définit leurs obligations pour connecter progressivement en très haut débit mobile la totalité de la population française et des territoires d'ici 2030¹¹⁵⁵.

Le PFTHD et les efforts de l'Arcep semblent avoir porté leurs fruits. La France est l'un des pays de l'OCDE dont la connexion à la fibre optique a le plus progressé entre 2019 et 2021 : la part de la fibre optique dans les connexions Internet haut débit est passé de 24% à 46% sur cette période, soit une hausse de 22% en deux ans, contre une hausse moyenne d'environ 7% dans l'OCDE sur cette période (passant en moyenne de 28 à 35%)¹¹⁵⁶. Au dernier trimestre 2021, la part des abonnements très haut débit dépasse la part des abonnements haut débit ; et au troisième trimestre 2022, le parc actif 4G connecte plus d'équipements (69,7 millions) que le parc actif 3G (69,3 millions)¹¹⁵⁷.

Au Royaume-Uni, l'action publique est intervenue plus tardivement qu'en France pour généraliser l'accès haut débit. En 2003, l'Ofcom régule l'accès haut débit, non pas dans le sens d'une telle généralisation, mais en suivant quatre objectifs tournés vers la libre concurrence et l'investissement dans les technologies haut débit : (a) une concurrence efficace et durable dans la fourniture de réseaux et de services haut débit ; (b) des mesures correctives rapides et fermes contre les pratiques anticoncurrentielles ; (c) un niveau élevé de sensibilisation des consommateurs à la nature des services haut débit ; et (d) un cadre réglementaire propice à

¹¹⁵² Arcep, Décision n° 2009-1106 du 22 décembre 2009 précisant, en application des articles L. 34-8 et L. 34-8-3 du code des postes et des communications électroniques, les modalités de l'accès aux lignes de communications électroniques à très haut débit en fibre optique et les cas dans lesquels le point de mutualisation peut se situer dans les limites de la propriété privée

¹¹⁵³ Par ex., Arcep, Décision n° 2010-1312 du 14 décembre 2010 précisant les modalités de l'accès aux lignes de communications électroniques à très haut débit en fibre optique sur l'ensemble du territoire à l'exception des zones très denses

¹¹⁵⁴ Les obligations sont les suivantes : « 1. améliorer la qualité de réception sur l'ensemble du territoire, et particulièrement dans les zones rurales (...) ; / 2. démultiplier le rythme des programmes ciblés d'amélioration de la couverture et dans ce cadre construire chacun au moins 5000 nouveaux sites sur tout le territoire, parfois mutualisés, qui iront désormais au-delà des zones dites "blanches" [zones dépourvues de couverture mobile] et dont la charge sera désormais intégralement prise par les opérateurs ; / 3. (...) apporter [la réception en 4G] à plus d'un million de Français sur 10 000 communes, en équipant en 4G tous les sites mobiles ; / 4. accélérer la couverture des axes de transport, afin que les principaux axes routiers et ferroviaires soient couverts en 4G. Cette obligation s'applique seulement aux lauréats de la procédure en bande 1800 MHz ; / 5. généraliser la couverture téléphonique à l'intérieur des bâtiments, notamment en proposant à leurs clients disposant d'un terminal compatible avec la voix sur Wifi », v. Arcep, « "New Deal" mobile », 25 oct. 2018

¹¹⁵⁵ Arcep, « Les obligations de déploiement des opérateurs », mis à jour le 30 mai 2023

¹¹⁵⁶ GAUDIAUT Tristan, « Fibre optique : quels pays ont les plus avancés ? », Statista, 28 juin 2023

¹¹⁵⁷ Arcep, « Marché des communications électroniques en France – Les chiffres au 4^{ème} trimestre 2022 », m.àj le 6 avr. 2023

l'investissement dans la large bande et le déploiement dans les régions reculées du pays¹¹⁵⁸. En 2009, le gouvernement britannique mandate un courtier indépendant du spectre, l'homme d'affaires Kip Meek spécialisé dans les médias et les communications électroniques, pour formuler des recommandations dans le sens d'un déploiement de l'accès haut débit au Royaume-Uni¹¹⁵⁹. Parmi les solutions proposées par le courtier, le gouvernement retient la suivante : étendre les fréquences exploitables par trois opérateurs en attribuant à chacun d'entre eux 2x10 MHz supplémentaires sur la bande 800 MHz (utilisée pour la 3G)¹¹⁶⁰. De cette façon, les trois opérateurs pourront transporter un plus gros volume de données via leurs réseaux 3G, ce qui conduit le courtier à proposer d'étirer les obligations de couverture de ces opérateurs pour couvrir jusqu'à 99% de la population à une vitesse haut débit spécifiée par l'Ofcom (par ex. 2 Mbit/s). Le courtier proposait par ailleurs une autre solution, attribuant à un seul opérateur 2x20 MHz sur la bande 800 MHz. Cette solution aurait certes accéléré la vitesse du trafic par rapport à la solution retenue, mais le gouvernement l'a écartée au motif qu'une « *diminution de l'intensité concurrentielle (...) en résulterait* »¹¹⁶¹.

En 2010, dans le cadre du Broadband Delivery Programme engagé entre 2011/2012 et 2014/2015, le gouvernement britannique crée le Broadband Delivery UK (BDUK, devenu Digital Building UK) au sein du ministère de la culture, des médias et des sports. Cette institution est chargée de cinq missions : supporter le développement de l'économie numérique au Royaume-Uni, y compris dans les zones rurales ; garantir dans le Royaume-Uni le meilleur très haut débit d'Europe d'ici 2015 ; assurer l'accès à internet haut débit pour toutes les communautés du Royaume-Uni d'ici 2015 ; veiller à l'utilisation efficace des fonds pour la fourniture de services haut débit et très haut débit ; et assister les autres initiatives gouvernementales pour augmenter les capacités d'accès des utilisateurs aux services haut débit¹¹⁶². Ce programme, qui repose sur une allocation gouvernementale de 530 millions £ pour stimuler les investissements privés, espère garantir un accès universel aux services haut débit d'ici 2015. Reprenant ainsi les recommandations du courtier faites en 2009, le gouvernement exige une vitesse minimale de 2 Mbit/s, et priorise la couverture haut débit en zones rurales¹¹⁶³. En 2015, l'Ofcom fixe à 10 Mbit/s le débit minimal devant être fourni par les services universels BT et KCOM, de façon que l'accès haut débit devient une composante du service universel au Royaume-Uni¹¹⁶⁴. Bien que, depuis 2006, BT soit contraint de fournir des tarifs sociaux d'accès bas débit pour les consommateurs à faible revenus ou bénéficiaires de certaines aides de l'État, il faudra attendre 2021 pour que BT propose des tarifs sociaux (à 15£) d'accès haut débit pour les bénéficiaires du crédit universel ou d'un crédit de pension¹¹⁶⁵. En 2022, à l'issue d'une négociation de l'Ofcom,

¹¹⁵⁸ Oftel, *Annual report 2003*, p. 19-20

¹¹⁵⁹ « Report of Independent Spectrum Broker published », *Thomson Reuters – Practical Law Competition*, mai 2009 ; Arcep, « Les titres de la presse du mardi 20 octobre 2009 », 20 oct. 2009

¹¹⁶⁰ Department for Business Innovation & Skills et Department for Culture, Media & Sport, « Digital Britain. Final Report », juin 2009, p. 76

¹¹⁶¹ *Ibid.*

¹¹⁶² Department for Science, Innovation & Technology et Department for Culture, Media & Sport, « BDUK Broadband Delivery Project », 9 mars 2011 ; Department for Digital, Culture, Media & Sport, « Broadband Delivery Programme: Delivery Model », sept. 2011

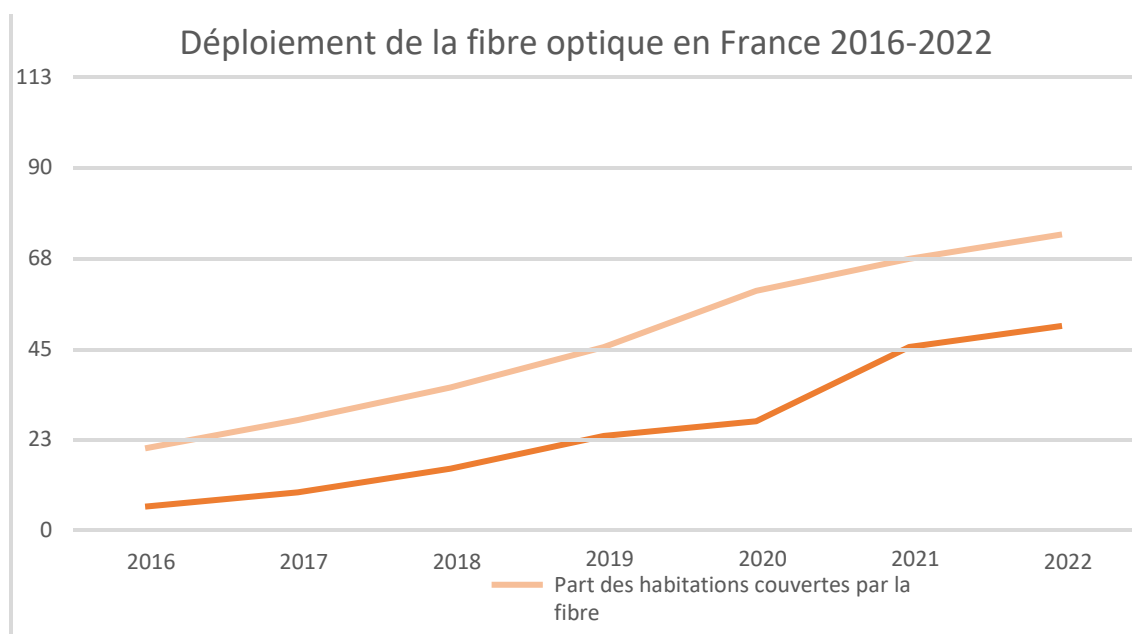
¹¹⁶³ Ofcom, « The availability of communications services in the UK », mai 2013, p. 71s.

¹¹⁶⁴ Ofcom, « Designing the broadband universal service obligation », avr. 2016

¹¹⁶⁵ Ofcom, « Retail Price Controls », 19 juil. 2006 ; SNELLING David, « Millions of BT customers offered budget broadband as new plan launches today », *Daily Express*, 29 juin 2021

du gouvernement et des opérateurs, la majorité des opérateurs s'engagent à fournir des tarifs sociaux haut débit après une année de hausse des tarifs non-sociaux¹¹⁶⁶.

Quant à l'extension de l'accès très haut débit, elle a été bien moins dynamique au Royaume-Uni qu'en France durant la décennie 2010. Depuis la fin des années 2000, BT fut le premier opérateur britannique à déployer la connexion par fibre optique, mais en se limitant aux modes de connexion FTTC (Fiber-to-the-curb, connexion de la fibre aux trottoirs à proximité des habitations) et FTTP (Fiber-to-the-premises, connexion de la fibre aux locaux) à défaut du mode FTTH (Fiber-to-the-home, connexion de la fibre aux habitations)¹¹⁶⁷. Le premier plan national de déploiement du très haut débit, le « Project Gigabit » est lancé en novembre 2020¹¹⁶⁸. Il consacre 5 milliards £ à cette tâche, dont 210 millions pour la couverture rurale et 110 millions pour connecter 7 000 cabinets de médecins généralistes, bibliothèques et écoles ruraux. En mars 2021, la veille de l'annonce officielle du Project Gigabit, l'Ofcom annonce qu'il ne régulera pas les prix sur le haut-débit en fibre optique avant 2031, dans le but de permettre aux opérateurs de reporter les prix de la fibre sur l'abonnement et ainsi de construire plus rapidement les infrastructures de fibre¹¹⁶⁹. Le retard britannique dans le déploiement du haut et du très haut débit se répercute sur la vitesse du trafic au Royaume-Uni : en mars 2022, le débit moyen au Royaume-Uni s'établissait à 59,4 Mbit/s sur une période de 24h, contre un débit moyen de 94 Mbit/s en France la même année¹¹⁷⁰.



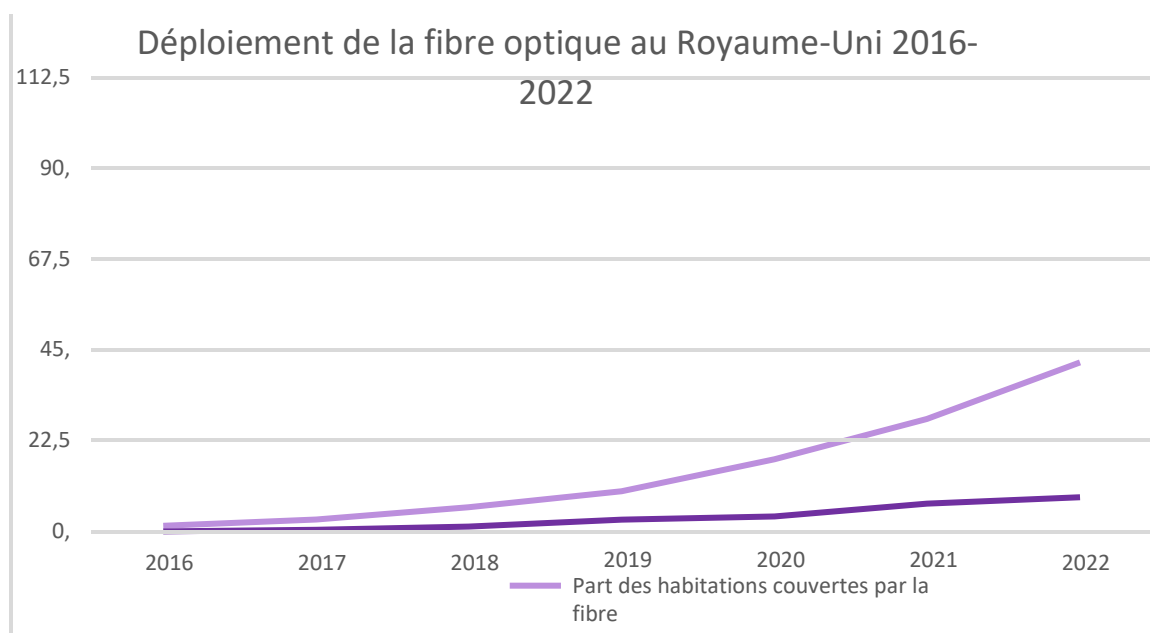
¹¹⁶⁶ JACKSON Mark, « Broadband ISPs and Mobile Operators Agree UK Cost-of-Living Plan », *ISP Review*, 27 juin 2022

¹¹⁶⁷ Ofcom, « Review of the wholesale broadband access markets », juin 2014, p. 11

¹¹⁶⁸ JACKSON M., « Gov Starts GBP5bn UK Gigabit Broadband and Voucher Schemes UPDATE », *ISP Review*, 19 mars 2021 ; Department for Digital, Culture, Media & Sport et DOWDEN Oliver, « Government launches new £5bn "Project Gigabit" » (communiqué de presse), 19 mars 2021 ; « Can private companies really help drive the roll-out of full fibre connectivity in 2021? », sur *Vxfiber.com*, 15 fév. 2021 (compagnie technologique suédoise spécialisée dans la construction et l'exploitation de la fibre)

¹¹⁶⁹ HUGHES Matthew, « Ofcom says no price controls on full-fibre broadband until 2031, giving BT's Openreach the kick to 'build like fury' », *The Register*, 18 mars 2021

¹¹⁷⁰ Ofcom, « UK Home Broadband Performance », oct. 2022 ; Arcep, « L'état d'internet en France. Edition 2023 », juil. 2023, p. 19-20



La part des habitations couvertes par la fibre optique indique le pourcentage d’habitations qui ont accès à la fibre, mais pas le pourcentage d’habitations qui y accèdent effectivement (*i.e.* qui paient un abonnement fibre)¹¹⁷¹. Inversement, la part de la fibre optique dans les connexions haut et très haut débit indique la part du trafic qui provient effectivement du transport par fibre optique, *i.e.* la part des requêtes qui sont effectivement émises par des abonnés à la fibre¹¹⁷².

En 2022, la France couvrait 74% des habitations en fibre optique, contre 42% au Royaume Uni. Surtout, la fibre représentait 51,3% du trafic haut et très haut-débit en France, contre seulement 8,6% au Royaume-Uni. On constate que, en France, la part de la fibre dans trafic haut et très haut débit a suivi une progression assez alignée sur la progression de la part des habitations couvertes par la fibre. Inversement, au Royaume-Uni, la progression de la part de la fibre dans le trafic national est beaucoup plus lente que la progression de la part des habitations couvertes. Cela signifie que, au Royaume-Uni, l’écart se creuse très exponentiellement entre le nombre de personnes ayant accès à la fibre et le nombre de personnes qui y accèdent effectivement. On explique cette différence avec la France notamment par les prix très élevés des abonnements britanniques, voire dissuasifs, sur lesquels les opérateurs

¹¹⁷¹ On a obtenu les chiffres rapportés en croisant les données de l’Arcep et de l’Ofcom : Ofcom, « Connected Nations 2016 », 16 déc. 2016 ; Ofcom, « Connected Nations 2017 », 15 déc. 2017 ; Ofcom, « Connected Nations 2018 », 18 déc. 2018 ; Ofcom, « Connected Nations 2019 », 20 déc. 2019 ; Ofcom, « Connected Nations 2020 », 19 déc. 2020 ; Ofcom, « Connected Nations 2021 », 16 déc. 2021 ; Ofcom, « Connected Nations 2022 », 15 déc. 2022 ; Arcep, « Observatoire Haut et Très Haut Débit : abonnements et déploiements. Les chiffres du 4ème trimestre 2017 », m^{ai} le 8 mars 2018 ; Arcep, « Marché du haut et du très haut débit fixe. Les abonnements à la fibre optique désormais majoritaires en France », Communiqué de presse, 8 sept. 2022

¹¹⁷² Les chiffres rapportés sont fournis par l’OCDE : OCDE, « Chapter 3. Access and connectivity » in *OECD Digital Economy Outlook 2020*, 2020 ; GAUDIAUT Tristan, « Fibre optique : quels pays sont les plus avancés ? », *Statista*, 28 juin 2023 ; « Statistiques du haut débit de l’OCDE », sur *oecd.org*, 23 fév. 2023

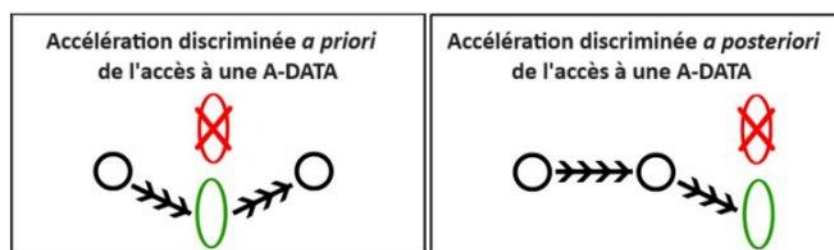
répercutent les coûts du déploiement de la fibre¹¹⁷³. Cette répercussion sur les prix facilite le déploiement de la fibre (couverture), mais réduit la clientèle potentielle de tels abonnements – *a fortiori* sans contrôle des prix par l’Ofcom.

En somme, la régulation britannique semble avoir été plus efficace que celle française pour ce qui est du raccordement et de la décentralisation du réseau – grâce à une régulation et à une libéralisation du marché bien plus précoce qu’en France. En revanche, la régulation française semble avoir été plus efficace que celle britannique pour ce qui est de l’accélération non-discriminée du trafic – grâce à une régulation nationale plus précoce qu’au Royaume-Uni, à un plan de coordination territoriale public-privé et à des investissements publics trois fois plus massifs.

Paragraphe 2 – Techniques basées sur le trafic pour augmenter spécifiquement l’accès aux A-DATA

Parmi les techniques d’augmentation qui reposent sur le trafic et qui permettent de cibler l’accès à des R-DATA, on étudiera l’accélération discriminée du trafic (A) et la redirection du trafic vers une R-DATA pratiquée dès l’acheminement (B), qu’on distinguera de la redirection du trafic pratiquée dès le stockage de données (C).

A) L’accélération discriminée de l’accès à une A-DATA dès la transmission de données



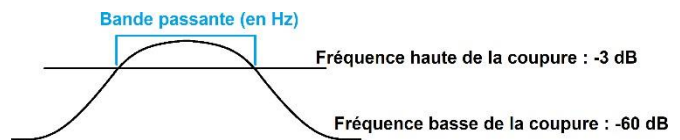
On appelle « accélération discriminée de l’accès à une A-DATA » la technique qui consiste à stimuler la vitesse du trafic à destination d’une ou plusieurs données admises par le régulateur. Tandis que l’accélération non-discriminée profite à toute requête indépendamment de sa destination, l’accélération discriminée accroît seulement la vitesse des requêtes destinées à une ou plusieurs A-DATA.

On voit deux principaux avantages à l’accélération discriminée. Premier avantage : par rapport à l’accélération non-discriminée, **l’accélération discriminée permet de privilégier spécifiquement l’accès à une ou plusieurs A-DATA**, au détriment des autres A-DATA et surtout des R-DATA dont l’accès n’est pas accéléré. L’accélération discriminée peut ainsi

¹¹⁷³ En 2020, les internautes français dépensaient en moyenne 33,1€/mois pour une connexion fixe à internet et 14,4€/mois pour une connexion mobile, soit en moyenne 47,5€/mois : v. Arcep, Observatoire des marchés des communications électroniques, « Les services de communications électroniques en France. 1^{er} trimestre 2022 », 7 juil. 2022 ; Arcep, « Marché des communications électroniques en France – Les chiffres au 4^{ème} trimestre 2021 », māj le 7 avril 2022. La même année, les internautes britanniques dépensaient en moyenne 40,87£/mois pour une connexion fixe à internet et 38,22£/mois pour une connexion mobile, soit en moyenne 79,1£ pour un accès fixe et mobile : TAYLOR Petroc, « Average monthly household spend on telecommunication services in the United Kindom from (UK) 2007 to 2021 », *Statista*, 29 juin 2023

renforcer la centralisation si les requêtes accélérées sont celles destinées à des nœuds centraux. Par exemple, si les opérateurs accélèrent le trafic à destination de très grands services partenaires (YouTube, Amazon, Netflix...), l'accès aux applications centrales sera privilégié au détriment des autres applications, favorisant un peu plus encore l'essor de nœuds déjà centraux. Dans ce sens, en combinant plusieurs techniques restriction et d'augmentation, il est alors possible de centraliser fortement un réseau (en restreignant la diversité des voies d'accès aux données) puis d'en faire un système à trois vitesses : un faible débit accordé aux R-DATA (ralentissement de l'accès à une R-DATA) ; un bon débit accordé à la plupart des A-DATA (accélération non-discriminée de l'accès à internet) ; et un excellent débit accordé aux A-DATA que le régulateur souhaite promouvoir (accélération non-discriminée de l'accès à une A-DATA). Une telle combinaison aboutirait à un réseau fortement centralisé en faveur de l'accès aux A-DATA, discriminant l'accès aux R-DATA.

Deuxième avantage : **l'accélération discriminée permet d'ajuster la répartition de la vitesse du trafic pour garantir un fonctionnement correct d'internet.** En effet, la vitesse du trafic est étroitement liée à la notion de bande passante. La bande passante désigne l'intervalle de fréquences dans lequel le signal électrique faiblit moins par rapport à une valeur déterminée. Par exemple, pour un son qui est régulièrement coupé, la bande passante désigne l'intervalle entre la fréquence de coupure haute (-3 décibels) et la fréquence de coupure basse (-60 décibels).

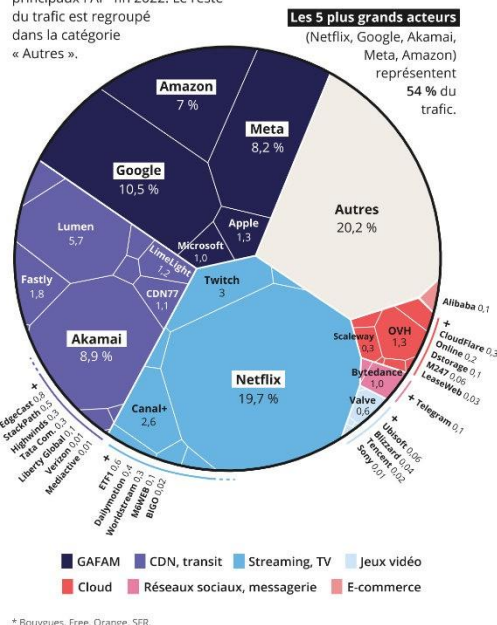


Par extension, dans le cas d'internet, le concept de bande passante est employé pour décrire le volume maximal de données qui peut être transmis d'un point A à un point B en un temps prédéfini. Plus la bande passante est élevée, plus est volumineuse la quantité de données pouvant être transmise dans un laps de temps réduit. Ainsi, une voie d'accès dont le débit passe de 10 Mbit/s à 50 Mbit/s connaît une augmentation de sa bande passante.

Il est établi depuis de nombreuses années que les applications en ligne de streaming vidéo (*i.e.* de partage ou de distribution de vidéos en flux continu comme YouTube, Netflix, Twitch...) sont très consommatrices de bande passante, en raison du flux continu de données et de la haute définition de la vidéo. On rapporte ci-contre la représentation graphique, par l'Arcep, des services les plus consommateurs de bande passante en France fin 2022, d'après les données des principaux opérateurs français¹¹⁷⁴. Si les opérateurs risquent la surcharge de leurs infrastructures, ils peuvent techniquement réduire la bande passante qu'ils accordent à un service sur internet, et augmenter la bande passante qu'ils accordent à des services nécessaires à l'organisation sociale.

Décomposition selon l'origine du trafic vers les clients des principaux FAI en France (fin 2022)

Pourcentage du trafic entrant au point d'interconnexion de 39 acteurs liés au transport ou à la production de contenu déclarés par les principaux FAI* fin 2022. Le reste du trafic est regroupé dans la catégorie « Autres ».



Par exemple, on a vu que la pandémie de Covid19 a favorisé l'essor des applications de télétravail (Microsoft Teams, Zoom, Google Drive, Evernote...). Or, si une application en ligne voit croître le nombre de ses utilisateurs, est du même coup amplifié le volume de données transmis vers et par cette application. Autrement dit, plus un service en ligne gagne d'utilisateurs, plus ses besoins de consommation de bande passante sont élevés – bien que le nombre d'utilisateurs ne soit pas le critère le plus déterminant. Imaginons que les applications de télétravail représentaient 0,1% de la bande passante avant la pandémie, mais que leurs besoins de consommation de bande passante s'élèvent à 2% après la pandémie. Si les opérateurs ne leur accordent que 0,5% de la bande passante, le trafic destiné à ces applications sera très lent car le débit binaire dont elles bénéficieront ne sera pas à la mesure du volume de données qu'elles consomment. *A contrario*, si les opérateurs leur accordent 2% de la bande passante, la vitesse du trafic destiné à ces applications sera adaptée à leurs besoins de consommation de données.

Pour que la vitesse de trafic soit égale d'un service en ligne à un autre, chaque service doit alors bénéficier d'une part de la bande passante proportionnée à la quantité de données qu'il consomme. En principe, les opérateurs n'ont pas à répartir le pourcentage de bande passante pour égaliser la vitesse d'accès : la bande passante des opérateurs suffit pour que chaque service puisse en profiter selon ses besoins. En revanche, lorsque la capacité de la bande passante ne suffit plus aux besoins de consommation de données de tous les services en ligne, les infrastructures des opérateurs risquent la surcharge – quantité de données excédant les capacités de transmission des opérateurs. En cas de surcharge, les applications de télétravail ne pourront pas atteindre les 2% de bande passante dont elles ont besoin pour fonctionner correctement. Les opérateurs peuvent dans ce cas réduire la bande passante accordée à des services de divertissement par vidéo (Netflix, YouTube, Amazon Prime Video...) et attribuer aux applications de télétravail la bande passante ainsi récupérée. Concrètement, si les applications de télétravail ne

¹¹⁷⁴ Arcep, « L'état d'internet en France. Rapport d'activité », juil. 2023, p. 42

représentent que 0,5% de la bande passante alors que leurs besoins s'élèvent à 2%, les opérateurs pourront leur attribuer les 1,5% nécessaires en les retirant à Netflix (passant de 19,7% à 18,2%). Le trafic à destination de Netflix sera dans ce cas ralenti afin d'accélérer l'accès aux applications de télétravail.

Dans l'Union européenne, le principe de neutralité interdit aux opérateurs de discriminer l'accès aux services (en l'espèce discriminer l'accès à Netflix au profit des applications de télétravail), mais la directive européenne pour un internet ouvert admet que les impératifs de fonctionnement du réseau puissent justifier une telle discrimination¹¹⁷⁵. Même face à un risque de surcharge, l'accélération discriminée est toutefois très peu prise en compte dans l'UE, sinon en ultime recours : craignant une surcharge du réseau liée à la pandémie, et pour garantir un accès de qualité aux applications de télétravail, le Commissaire européen au marché intérieur Thierry Breton appelait les plateformes vidéo à réduire la définition des vidéos plutôt qu'à réduire la bande passante consacrée à ces plateformes au profit des applications de télétravail ; de même, le Secrétaire d'État français chargé du numérique Cédric O a préféré retarder le lancement de Disney+ sur le marché français plutôt que de réguler la répartition de la bande passante¹¹⁷⁶. Bien que l'accélération ou le ralentissement discriminés puissent être efficaces pour garantir le bon fonctionnement du réseau en cas de surcharge, l'UE est particulièrement réticente à l'idée de discriminer le trafic. La solution européenne – réduction de la définition de la vidéo – était probablement plus pertinente, car elle permet effectivement d'économiser la consommation de la bande passante sans léser la vitesse d'accès aux services de streaming vidéo.

On reconnaît en revanche deux inconvénients à la technique de l'accélération discriminée. Premier inconvénient : contrairement à la volonté du régulateur, **l'accélération discriminée peut profiter aux R-DATA ou desservir les A-DATA**. L'accélération discriminée peut d'abord profiter aux R-DATA. En effet, si l'accès à un service est accéléré, toutes les données hébergées par ce service le sont aussi, y compris les R-DATA (contenus haineux, fausses informations, harcèlement, consultation de contenus pornographiques par des mineurs...). De même, si l'accès à une page web spécifique (URL) est accéléré, une telle accélération peut certes représenter un atout pour cette page qui gagnera en popularité face aux pages web concurrentes plus lentes ; mais il deviendra alors intéressant pour un cyberattaquant d'utiliser un logiciel malveillant pour infecter la page web promue par le régulateur, et ainsi diffuser rapidement son logiciel malveillant auprès d'un grand nombre de visiteurs. Dans les deux cas étudiés, l'accélération discriminée au bénéfice des A-DATA peut en réalité faciliter l'accès aux R-DATA, et contribuer à leur vaste diffusion (en favorisant l'essor de données centrales dont l'accès est spécialement accéléré).

L'accélération discriminée peut ensuite desservir les A-DATA promues par le régulateur. En effet, dans les cas étudiés, l'accélération discriminée repose sur le destinataire de la requête (nom de domaine, URL, adresse IP destinataire...). Toutefois, elle peut aussi reposer sur les autres informations contenues dans la requête de l'utilisateur (protocoles utilisés, textes, images, vidéos ou sons émis, adresse IP émettrice...). Dans ce dernier cas, l'accélération discriminée est pratiquée au moyen d'un filtrage des requêtes : est alors privilégiée la transmission des seules requêtes porteuses des A-DATA promues (protocoles utilisés comme HTTPS, contenus d'informations que le

¹¹⁷⁵ Règlement européen 2015/2120 dit « pour l'accès à un Internet ouvert », art. 3.3, b) et c)

¹¹⁷⁶ GAVOIS Sébastien, « On vous explique (simplement) comment fonctionnent les tuyaux d'Internet », *NextInPact*, 26 mars 2020

régulateur souhaite valoriser voire contenus de propagande...). Or, recourir au filtrage pour accélérer l'accès à certaines A-DATA implique les mêmes inconvénients que ceux relevés pour le filtrage, à savoir l'aggravation du risque de sur-filtrage ou de sous-filtrage. Dans l'hypothèse d'un sous-filtrage, sera accéléré l'accès à certaines A-DATA non promues par le régulateur, voire l'accès à certaines R-DATA. Dans l'hypothèse d'un sur-filtrage, ne sera pas accéléré l'accès à certaines A-DATA promues par le régulateur.

Deuxième inconvénient : **l'accélération discriminée de l'accès à une A-DATA voit ses effets neutralisés si les utilisateurs délaissent cette A-DATA**. En effet, on a vu que le risque de contournement est un inconvénient fréquent pour les techniques de restriction. Mais en présence d'une technique d'augmentation de l'accès, le problème du contournement se pose plus rarement : tandis que les utilisateurs ont généralement le choix entre contourner ou accepter une technique de restriction d'accès, ils ont en principe le choix entre délaisser ou adopter une technique d'augmentation d'accès. Concrètement, les utilisateurs ne peuvent pas contourner l'accélération de l'accès à un service ni même les techniques de décentralisation mises en œuvre, mais ils peuvent délaisser le service dont l'accès est accéléré ou les services décentralisés en ne les utilisant pas, au profit d'un service refusé par le régulateur ou d'un service central. Aussi, l'accélération discriminée vers un service que le régulateur souhaite promouvoir peut donner à ce service un avantage particulier s'il est en position de rivaliser sérieusement avec les principaux concurrents. *A contrario*, si le service dont l'accès est accéléré est en faible posture concurrentielle, la rapidité de la vitesse de connexion ne sera probablement pas un atout suffisant pour attirer les utilisateurs des grands services concurrents. Moins la A-DATA rassemblait d'utilisateurs avant de bénéficier d'une accélération discriminée, plus est important le risque de délaissement de l'accélération¹¹⁷⁷.

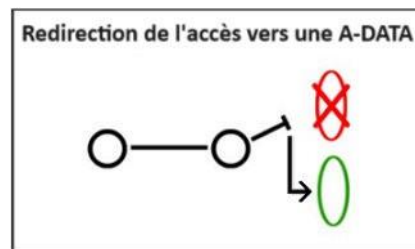
B) La redirection de l'accès vers une A-DATA depuis l'acheminement de données

1. Avantages de la redirection vers une A-DATA

On appelle « redirection de l'accès vers une A-DATA » la technique qui consiste à modifier la destination d'une requête pour rediriger vers une A-DATA le trafic initialement destiné à une R-DATA.

On reconnaît deux principaux avantages à la redirection d'une R-DATA vers une A-DATA. Premier avantage : la redirection **participe au bon fonctionnement du réseau**.

La redirection n'est pas en soi une technique d'augmentation, mais peut tout à fait être employée comme technique de restriction. Il en va ainsi de la redirection trou noir (ou redirection Null) qui consiste à rediriger le trafic vers une route trou noir, *i.e.* vers une route menant à des nœuds qui suppriment les données stockées sans en informer la source de ces données. Pour créer une route trou noir, il suffit à l'opérateur de configurer l'interface « Null » de ses routeurs¹¹⁷⁸. L'interface Null est une sorte de poubelle, une interface virtuelle qui supprime les paquets lui



¹¹⁷⁷ On verra que le risque de délaissement peut notamment être réduit en consacrant d'importants investissements au développement de la A-DATA concernée (pour que ladite A-DATA gagne d'autres qualités que sa vitesse d'accès), en insérant la A-DATA à une application très utilisée mondialement (pour l'exposer à un large public), en valorisant l'affichage de la A-DATA auprès des utilisateurs à l'aide d'algorithmes (pour augmenter sa visibilité)...

¹¹⁷⁸ VARGHESE Paul, « Null Interface », sur *Community.cisco.com*, 2 juil. 2009 māj le 1^{er} mars 2019

étant transmis. L'opérateur configure son interface Null pour lui renvoyer les paquets destinés aux réseaux privés listés lors de la configuration. De cette façon, tous les paquets adressés au réseau placé sur liste noire sont tous supprimés. La suppression du trafic destiné à ce réseau empêche l'accès, depuis les routeurs ainsi configurés, aux machines membres du réseau placé sur liste noire. La redirection Null peut donc être utile pour bloquer l'accès à certains réseaux entiers, mais elle est inadaptée pour cibler précisément une machine, un site web, un nom de domaine ou une adresse URL. Dans ces derniers cas, un blocage par identité <adresse IP :port>, par nom de domaine ou par URL sera plus adapté. La redirection Null est une technique de restriction d'accès à une R-DATA et non d'augmentation de l'accès à une A-DATA : les requêtes d'accès ne sont pas redirigées vers une donnée désirée par le régulateur, mais sont supprimées car non désirées par le régulateur.

Cependant, la redirection trou noir contribue aussi fondamentalement au bon fonctionnement du réseau. Elle est le plus souvent utilisée pour servir de poubelle aux erreurs qui circulent sur le réseau. Par exemple, lorsque des routeurs se transmettent par erreur un même paquet de manière répétée et infinie, le paquet est pris dans une boucle dont il ne peut sortir. Pour quitter sa boucle interminable, le paquet peut être redirigé vers l'interface Null d'un des routeurs, ce qui aura pour effet de mettre un terme à la boucle en supprimant le paquet¹¹⁷⁹. La redirection Null peut aussi se révéler très efficace contre les attaques par déni de service (DDoS, envoi excessif de requêtes à destination d'une ou de plusieurs machines cibles). Dans ce cas, tous les paquets IP – ceux légitimes comme ceux issus de l'attaque – sont redirigés vers une route trou noir. Il est aussi possible à l'administrateur du réseau de distinguer, dans une certaine mesure, les paquets légitimes de ceux illégitimes en configurant son routeur selon des critères de restriction qui différencient ces deux types de paquets¹¹⁸⁰.

On s'intéresse ici à l'emploi de la redirection à des fins d'augmentation de l'accès vers une A-DATA, et non à des fins de restriction de l'accès vers une R-DATA. On s'attarde précisément sur deux types de redirections vers une A-DATA dès l'acheminement : les redirections ICMP et les redirections de ports. Le premier type de redirections repose sur l'ICMP (*Internet Control Message Protocol*), un protocole de communication accompagnant le protocole TCP/IP pour que les routeurs puissent se communiquer les messages d'erreur durant le trajet des paquets IP (*i.e.* des datagrammes IP). Entre autres dispositifs qu'il propose, l'ICMP permet à tout routeur de rediriger les requêtes et leurs réponses vers un autre routeur.

Une redirection ICMP n'est possible que si le commutateur Ethernet d'un réseau local connecte un même hôte (*i.e.* une même machine de stockage de données) à au moins deux passerelles différentes G1 et G2 (box, modem...). Concrètement, un hôte (par ex. un terminal) souhaite accéder à un hôte destinataire (par ex. un serveur) ; les données émises par ce terminal empruntent G1 (*Gateway 1*) pour être acheminées jusqu'à cette destination ; G1 vérifie sa table de routage, et constate que la passerelle G2 propose une route plus courte pour atteindre la destination ; G1 envoie un message appelé *ICMP Redirect* à l'hôte émetteur (le terminal) pour l'informer de ce que G2 propose le meilleur itinéraire ; puis G1 poursuit l'acheminement qu'il a commencé, en transmettant le premier paquet IP (*i.e.* le premier datagramme IP) vers sa destination ; maintenant que l'hôte émetteur est informé du bon itinéraire, au lieu d'adresser les paquets suivants à G1,

¹¹⁷⁹ « Use a Static Route to the Null0 Interface for Loop Prevention » [en ligne], Cisco, maj le 9 janv. 2023

¹¹⁸⁰ « Qu'est-ce que le routage blackhole DDoS » [en ligne], CloudFlare, consulté le 17 juil. 2023

il les adresse à la passerelle G2¹¹⁸¹. Le trafic, initialement transmis à G1, est alors redirigé vers G2 grâce à l'*ICMP Redirect*.

Les passerelles G1 et G2 doivent être connectées par le même commutateur pour pouvoir communiquer directement et donc générer les messages *ICMP Redirect*. Cette hypothèse concerne classiquement des réseaux d'entreprise, des réseaux de serveurs (datacenter), des réseaux universitaires ou des réseaux d'établissement de santé qui utilisent plusieurs adresses IP publiques, mais peut aussi tout à fait concerner un réseau domestique qui s'équipe d'au moins deux passerelles. La redirection ICMP permet non seulement d'optimiser le chemin de transmission des données sur internet, mais aussi d'économiser les ressources réseau (bande passante, puissance de calcul des processeurs des routeurs...). En d'autres termes, lorsqu'une requête provoque la R-DATA « consommation excessive de bande passante » ou la R-DATA « dépassement de la puissance de calcul des routeurs », la redirection ICMP permet de rediriger cette requête vers les A-DATA « diminution de la bande passante consommée » et « capacité suffisante des routeurs pour traiter les requêtes d'accès ».

Outre les redirections ICMP, l'acheminement peut aussi servir à des redirections de ports. On a vu que les ports internet sont les voies d'accès logiques (et non physiques) aux différents hôtes présents sur internet – le port 80 pour accéder aux services France, le port 443 pour les services HTTPS, le port 53 pour accéder au réseau DNS, le port 25 pour accéder aux services de messagerie, le port 179 pour l'accès au BGP (protocole d'échange de paquets IP entre les routeurs et de détermination de l'itinéraire le plus avantageux), ou encore les ports 20 et 21 pour l'accès au FTP (protocole de transferts de fichiers). Les 1023 premiers ports – réservés – sont attribués par l'IANA¹¹⁸².

La redirection de ports complète la capacité d'une machine d'accéder au réseau internet public par la capacité de la machine de devenir accessible à toute autre machine sur internet. On a déjà illustré le fait que les machines membres d'un réseau privé accèdent au réseau public grâce à leur passerelle, laquelle fait correspondre leurs adresses IP privées avec l'adresse IP publique de la passerelle (l'adresse IP privée d'un terminal est *traduite* en l'adresse IP publique de la passerelle pour transmettre des données sur le réseau public). Assurée par la passerelle, cette fonction de traduction d'une adresse IP privée en adresse IP publique est appelée fonction « NAT » (*Network Address Translation*). Tandis que la fonction NAT permet aux requêtes provenant d'un réseau interne d'être transmises vers le réseau externe, la fonction de redirection de ports permet aux requêtes provenant du réseau externe (public) d'être transmises vers une machine d'un réseau

¹¹⁸¹ La redirection ICMP est décrite par la RFC 792 ; v. aussi MEROLA Antonio, « Utilisation et abus sur le protocole ICMP », *Hakin9*, n° 2, 2006, p. 50 ; et « Comprendre les messages de redirection ICMP » [en ligne], Cisco, m^{ai} le 22 sept. 2022

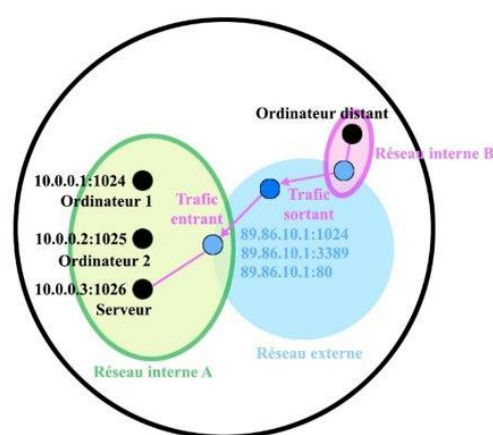
¹¹⁸² Par exemple, l'IANA a autorisé en février 2021 la société Alphabet à déployer sur les ports 80 et 443 son protocole QUIC (Quick UDP Internet Connections Protocol), un protocole qui permet aux utilisateurs d'accéder plus rapidement aux services en ligne depuis le navigateur web Chrome : entrée « QUIC », sur *Iana.org/assignments*, m^{ai} le 31 mai 2023. Pour accélérer le chargement des pages web, le protocole QUIC n'exige pas du serveur qu'il confirme la réception du message à l'auteur de la requête, comme c'est traditionnellement le cas ; dans le cas de QUIC, la requête vérifie elle-même la bonne réception du message par le serveur, ce qui évite au message de confirmation de devoir faire le chemin jusqu'à l'auteur de la requête. Ce protocole réduit donc la bande passante consommée, économise les ressources réseau, contribue à décongestionner le réseau, et diminue le temps de chargement d'une page web. V. notamment « QUIC : le protocole de transport Internet basé sur UDP » [en ligne], IONOS, 1^{er} mars 2023.

interne. Pour ce faire, une machine membre d'un réseau interne doit être identifiable depuis l'extérieur du réseau. Or, on sait que les machines membres d'un réseau privé sont identifiées par des adresses IP privées, invisibles à l'extérieur du réseau privé. Afin d'identifier une machine membre d'un réseau privé depuis le réseau externe, la redirection de ports utilise donc deux ressources qui peuvent être connues sur le réseau public : l'adresse IP publique de la passerelle à laquelle est connectée cette machine ; et le numéro de port utilisé pour communiquer avec cette machine.

Prenons l'exemple du réseau privé A, qui comporte deux ordinateurs et un serveur. Ces trois machines sont respectivement dotées des adresses IP privées suivantes : 10.0.0.1 (1^{er} ordinateur) ; 10.0.0.2 (2^e ordinateur) ; 10.0.0.3 (serveur). L'administrateur du réseau A configure sa passerelle d'abord pour attribuer un port local au premier ordinateur (port 1024), au second ordinateur (port 1025) et au serveur (port 1026). Au sein du réseau privé, les ordinateurs et le serveur sont donc chacun identifiables par les combinaisons « adresse IP privée :port » suivantes : 10.0.0.1 :1024 (1^{er} ordinateur) ; 10.0.0.2 :1025 (2^e ordinateur) ; 10.0.0.3 :1026 (serveur). L'administrateur du réseau A configure ensuite sa passerelle pour que, dans sa table de routage, chaque port local attribué dans le réseau privé (1024, 1025, 1026) corresponde à des ports accessibles depuis le réseau extérieur (respectivement 1024, 3389 et 80). La table répertorie ainsi les correspondances :

Table de routage		
	Identification de la machine dans le réseau privé (combinaison <adresse IP privée :port>)	Identification de la machine dans le réseau public (combinaison <adresse IP publique :port>)
1 ^{er} ordinateur	10.0.0.1 :1024	89.86.10.1 :1024
2 ^e ordinateur	10.0.0.2 :1025	89.86.10.1 :3389
Serveur	10.0.0.3 :1026	89.86.10.1 :80

Si un ordinateur situé hors du réseau privé A souhaite accéder spécifiquement au serveur, il lui suffit d'adresser une requête à destination de 89.86.10.1 sur le port 80 (port France). Or, dans sa table de routage, la passerelle portant l'adresse IP publique 89.86.10.1 sait que le port 80 est associé à l'adresse privée 10.0.0.3, *i.e.* à l'adresse du serveur. Lorsqu'un internaute accède au site web hébergé par ce serveur, il adresse donc sa requête à l'adresse publique 89.86.10.1 en empruntant le port 80, et la passerelle redirigera la requête spécifiquement vers le serveur (accessible depuis cette adresse IP publique et ce port).



Si un ordinateur situé hors du réseau privé A souhaite accéder spécifiquement au serveur, il lui suffit d'adresser une requête à destination de 89.86.10.1 sur le port 80 (port France). Or, dans sa table de routage, la passerelle portant l'adresse IP publique 89.86.10.1 sait que le port

80 est associé à l'adresse privée 10.0.0.3, *i.e.* à l'adresse du serveur. Lorsqu'un internaute accède au site web hébergé par ce serveur, il adresse donc sa requête à l'adresse publique 89.86.10.1 en empruntant le port 80, et la passerelle redirigera la requête spécifiquement vers le serveur (accessible depuis cette adresse IP publique et ce port).

En somme, la redirection de ports consiste à remplacer une combinaison <adresse IP :port> par une autre. De nombreuses utilisations sont faites de la redirection de ports. Prenons ici l'exemple d'une entreprise qui héberge son site web sur un serveur. En plus de ce serveur, l'entreprise met à disposition de ses employés des ordinateurs qui fournissent des outils de travail (documents de l'entreprise et des employés comme des statistiques ou des graphiques, logiciels fournis par l'entreprise comme les suites bureautiques Adobe ou Microsoft, bases de données payantes comme Dalloz, Semrush ou BVDInfo, environnements de développement intégré – logiciels qui aident le programmeur à développer des logiciels – comme SlickEdit ou Eclipse IDE...). Les ordinateurs professionnels et le serveur qui héberge le site web de l'entreprise sont connectés à internet par la même passerelle – la passerelle 89.86.10.1 pour reprendre notre exemple. Les internautes qui accèdent au site web de l'entreprise y accéderont en empruntant le port 80 à destination de la passerelle 89.86.10.1. En revanche, les employés qui souhaitent accéder à distance (par ex. depuis chez eux) aux ordinateurs professionnels de l'entreprise emprunteront cette fois le port 3389 à destination de la même passerelle pour utiliser leurs outils de travail en tout lieu – le port 3389 est utilisé notamment pour le RDP (*Remote Desktop Protocol*), un protocole de Microsoft qui permet de donner accès à distance à un Bureau d'ordinateur Windows. Le port utilisé (80 ou 3389) permettra donc de distinguer la machine (serveur ou ordinateur professionnel) à laquelle sera destinée une requête provenant de l'extérieur¹¹⁸³.

De même, il est possible de réserver l'accès d'un port à certains réseaux privés définis. Pour rester sur notre exemple, l'entreprise peut réserver l'accès du port 3389 via la passerelle 89.86.10.1 aux seuls réseaux domestiques de ses salariés. L'administrateur du réseau doit dans ce cas configurer sa passerelle, pour ajouter manuellement les réseaux privés de ses salariés autorisés à accéder aux ordinateurs professionnels¹¹⁸⁴. La redirection de ports est aussi exploitée par certains VPN pour rediriger les paquets IP vers des ports qui ne transmettent pas les informations sur les adresses IP¹¹⁸⁵. De cette manière, les paquets peuvent être transmis sur le réseau sans que soit identifiable l'adresse IP de leur auteur.

¹¹⁸³ Soft4Europe, « TS2log – Configuration des box ADSL. Redirection des ports TCP », sur *Soft4Europe-france.com*, déc. 2018. Soft4Europe est une entreprise évaluant la faisabilité technique des projets qui lui sont soumis par ses clients. En l'espèce, elle explique comment elle utilise la redirection de ports pour permettre un accès distinct à son site web (via le port 80) et à ses ordinateurs professionnels (via le port 3389).

¹¹⁸⁴ Par ex., la commande `pass in egress proto tcp from 203.0.113.14 to any port 80 rdr-to 89.86.10.1` indique que seul le réseau portant l'adresse IP publique 203.0.113.14 peut accéder à la passerelle 89.86.10.1 via le port 80. Ou encore, la commande `pass in egress proto tcp from 198.51.100.89 to any port 80 rdr-to 89.86.10.1` indique que seul le réseau 198.51.100.89 peut accéder à la passerelle 89.86.10.1 via le port 3389. Inversement, la commande `pass in egress proto tcp from any port 80 rdr-to 89.86.10.1` indique que n'importe quel réseau peut accéder à la passerelle 89.86.10.1 via le port 80. V. « PF – Traffic Redirection (Port Forwarding) », *Openbsd.org*, consulté le 17 juil. 2023 [OpenBSD est un système d'exploitation libre, très attaché au chiffrement]

¹¹⁸⁵ MUJOVIĆ Vuk, « Qu'est-ce qu'une redirection de port et à quoi sert-elle ? », *Le-vpn.com*, nov. 2018

La redirection de ports sert donc fondamentalement à rendre une machine spécifique identifiable et donc accessible depuis le réseau public. Par extension, elle permet de limiter à certains réseaux nommément désignés l'accès à un site web ou à des outils professionnels, d'anonymiser les paquets de données, ou encore de bloquer/filtrer depuis l'acheminement l'accès à une machine spécifique à partir de son identité <adresse IP :port>. En raison de son intérêt fondamental, la redirection de ports est nécessaire pour assurer le bon fonctionnement du réseau.

Deuxième avantage de la technique de redirection : lorsque l'accès à une R-DATA est redirigé vers une A-DATA, **l'accès à cette R-DATA provoque une hausse de l'échelle de diffusion de la A-DATA sans contribuer à l'échelle de diffusion de cette R-DATA**. À notre connaissance, cette technique est la seule technique de régulation interne à présenter cet avantage d'amplifier l'échelle de diffusion d'une A-DATA tout en réduisant celle de la R-DATA accédée. On a vu par exemple que la redirection ICMP évite l'accès à une passerelle mal positionnée dans la transmission de données (R-DATA) au profit d'une passerelle mieux positionnée et d'une route moins dépensière en ressources réseaux (A-DATA). Grâce à la redirection vers une A-DATA, l'accès à une R-DATA est ainsi converti en un accès à une A-DATA.

La redirection DNS est une autre illustration typique de cet avantage. Une redirection DNS consiste à réacheminer le trafic destiné à une adresse IP, une adresse URL ou un nom d'hôte d'autre vers une autre adresse IP (redirection par adresse IP et redirection MXE pour les serveurs de messagerie), une autre adresse URL (redirections URL) ou un autre nom d'hôte (redirection CNAME et redirection MX pour les serveurs de messagerie). Concrètement la redirection DNS par un routeur procède de la même manière que la redirection de ports. Elle fait correspondre une ou plusieurs adresses IP/URL/noms d'hôte destinataires à l'adresse IP/URL/nom d'hôte de la machine vers laquelle est redirigé le trafic. Par exemple, si la table de routage fait correspondre l'adresse IP destinataire 89.86.10.1 à l'adresse IP 210.30.15.1, le routeur transmettra au réseau 210.30.15.1 les paquets initialement destinés à 89.86.10.1 ; si le routeur fait correspondre le nom de domaine [Linkedin.com](https://www.linkedin.com) avec le nom de domaine [Copainsdavant.fr](https://www.copainsdavant.fr), le routeur transmettra à [Copainsdavant.fr](https://www.copainsdavant.fr) les paquets initialement destinés à [Linkedin.com](https://www.linkedin.com). La redirection DNS contribue au bon fonctionnement du réseau car elle donne au serveur DNS accédé par l'utilisateur (par ex. le serveur DNS hébergeant [facebook.com](https://www.facebook.com)) la possibilité de rediriger les données de l'utilisateur vers le serveur qui héberge le service correspondant à ce nom de domaine (par ex. le serveur hébergeant le réseau social Facebook). En d'autres termes, la redirection DNS permet d'abord à l'utilisateur d'accéder au service portant le nom de domaine accédé.

En plus de contribuer au bon fonctionnement du réseau, cette technique sert aussi à réduire l'échelle de diffusion de la R-DATA redirigée vers une A-DATA. En France, la redirection DNS d'une R-DATA vers une A-DATA devient un outil administratif de régulation depuis 2015. On a vu que, depuis 2014, l'OCLCTIC peut demander à l'hébergeur ou à l'éditeur d'un site web de supprimer les contenus terroristes ou pédopornographiques présents sur son site ; si l'hébergeur ou l'éditeur ne s'exécute pas dans un délai de 24h, l'OCLCTIC peut ordonner aux opérateurs français de bloquer l'accès à cet hébergeur ou à cet éditeur¹¹⁸⁶. Un décret d'application de 2015 précise les modalités de ce blocage. Les sites web à caractère terroriste

¹¹⁸⁶ Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, art. 12 insérant un art. 6-1 à la LCEN

ou pédopornographiques bloqués doivent rediriger l'utilisateur vers une page web du ministère de l'intérieur, informant le visiteur des motifs du blocage et des voies de recours contre ce blocage¹¹⁸⁷. De cette façon, au lieu d'accéder à la R-DATA « page pédopornographique », l'utilisateur sera redirigé vers la A-DATA « page d'information du ministère de l'intérieur ». Sont ici combinées une technique de restriction (blocage d'une R-DATA) avec une technique d'augmentation (redirection vers une A-DATA). Du fait de cette combinaison, la technique prévue par le décret de 2015 hérite des avantages du blocage, mais aussi de ses inconvénients à commencer par l'aggravation du risque de sur-blocage. Ainsi, en mai 2023, la police a transmis aux opérateurs des adresses génériques de comptes utilisateurs à bloquer sur la messagerie Telegram, plutôt que les adresses des conversations pédopornographiques en cause sur Telegram¹¹⁸⁸. De nombreux utilisateurs français de Telegram ont alors été redirigés vers la page d'information du ministère de l'intérieur. Le dispositif issu du décret de 2015 est repris par un décret de 2017 pour les jeux d'argent en ligne : les applications de jeu d'argent en ligne non-agrées par l'Autorité nationale des jeux sont désormais redirigés vers une page d'information de ladite Autorité¹¹⁸⁹.

Les redirections DNS et de ports permettent aussi de prioriser l'accès à certains services, par exemple en redirigeant le trafic destiné à un réseau social étranger (R-DATA) vers un réseau social national (A-DATA), ou bien en redirigeant le trafic destiné à une application en ligne privée (R-DATA) vers une application en ligne étatique (A-DATA), ou encore en redirigeant le trafic destiné à des jeux vidéo (R-DATA) vers des applications de télétravail (A-DATA). Dans tous ces cas, l'accès à la R-DATA redirigée provoque un accès à la A-DATA.

2. Inconvénients de la redirection vers une A-DATA

Inversement, on reconnaît deux principaux inconvénients à la redirection vers une A-DATA, *i.e.* deux failles pour mettre en échec une telle redirection. Premier inconvénient : **les redirections vers une A-DATA facilitent de nombreux troubles à la sécurité du réseau**. En effet, par son existence même, la redirection donne à quiconque la contrainte le pouvoir de rediriger le trafic vers une R-DATA au lieu d'une A-DATA. Un attaquant peut ainsi contrôler une redirection vers une A-DATA, et corrompre cette redirection pour réacheminer le trafic vers une R-DATA plus dangereuse encore que la R-DATA initialement évitée.

Par exemple, la redirection ICMP ouvre la voie aux attaques par redirection ICMP. Ce type d'attaque consiste à infecter un hôte (terminal ou serveur) à l'aide d'un logiciel malveillant qui modifie la table de routage de cet hôte pour rediriger le trafic vers une autre machine. Elle prend la forme d'une attaque *man-in-the-middle-host* (MITM), par laquelle l'attaquant intercepte voire modifie les requêtes et communications entre deux hôtes (par ex. entre deux terminaux, ou entre un terminal et un serveur). En corrompant la table de routage d'un hôte, l'attaquant peut donc se servir des redirections ICMP pour usurper l'adresse IP ou surveiller les données provenant des machines attaquées, pour détourner le trafic à destination de sa propre machine, à destination

¹¹⁸⁷ Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, art. 3

¹¹⁸⁸ UTERSINGER Martin et REYNAUD Florian, « Les adresses Telegram bloquées en France par erreur », *Le Monde*, 13 mai 2023

¹¹⁸⁹ Décret n° 2017-677 du 28 avril 2017 portant diverses dispositions relatives à la régulation des jeux en ligne, art. 2

d'une route trou noir dans le but d'empêcher la machine attaquée d'accéder à des réseaux tiers, ou encore à destination d'une machine cible dans le but de mener un DDoS¹¹⁹⁰. Les redirections ICMP contribuent certes à diminuer la consommation de bande passante et à optimiser l'utilisation de la puissance de calcul (R-DATA évitées), mais elles permettent aux attaquants de prendre le contrôle d'une très vaste part du trafic (R-DATA facilitée par la redirection). Pour des raisons de sécurité – et notamment limiter le risque d'une attaque DdoS, d'une usurpation d'adresse IP, d'un espionnage, d'un vol de données... – il est ainsi parfois conseillé aux administrateurs des serveurs de désactiver les redirections ICMP¹¹⁹¹.

Le problème est similaire pour la redirection de ports : une machine identifiable par son <adresse IP :port> est à l'écoute sur ce port, *i.e.* disponible à l'accès sur ce port. La redirection crée ainsi une voie publique d'accès à cette machine. La machine étant ouverte sur un port public, elle est très exposée au risque d'intrusion et donc d'attaques. Cette exposition peut être limitée grâce à plusieurs options – par exemple en filtrant les réseaux autorisés à accéder à la machine comme on l'a vu (technique de filtrage), ou encore en plaçant la machine accédée dans un réseau séparé appelé « zone démilitarisée » ou DMZ pour que la compromission de la machine n'étende pas ses effets au-delà de la DMZ (technique de décentralisation)¹¹⁹². Que l'on soit en présence d'une redirection de ports, ICMP ou de trou noir, on observe donc que l'existence d'une redirection vers une A-DATA rend possible sa manipulation pour mettre en danger la sécurité du réseau. C'est tout aussi vrai pour les redirections DNS, qui permettent à l'attaquant de réacheminer le trafic destiné à une adresse IP, un nom de domaine ou une adresse URL vers une autre adresse infectée par un logiciel malveillant. Il suffira alors à l'utilisateur d'accéder à l'adresse initialement redirigée pour télécharger le logiciel malveillant. La mise en danger de la sécurité du réseau est encore aggravée lorsqu'un grand nombre de redirections pointent vers un même nœud destinataire, auquel cas ce nœud destinataire devient central par les redirections qu'il concentre et représente alors un nœud critique dont dépendent de nombreuses machines.

Deuxième inconvénient : en plus de démultiplier les possibilités d'attaques, **les redirections vers une A-DATA démultiplient les possibilités de contourner une technique de restriction**. Par exemple, la redirection de ports peut être utilisée par certains VPN pour permettre au serveur VPN d'être en communication directe avec l'hôte utilisateur. Dans ce cas, l'application locale du VPN donne à l'utilisateur la possibilité d'ouvrir son terminal sur un port précis ; le serveur VPN et le terminal de l'utilisateur peuvent donc directement s'échanger des données sur ce port, de sorte que le tunnel de chiffrement entre le terminal et le serveur VPN est direct. De ce fait, le serveur VPN peut directement communiquer son adresse IP à destination du terminal, le terminal peut substituer sa propre adresse IP par celle du serveur VPN, et tout cela en contournant les règles NAT de la passerelle de l'utilisateur (*i.e.* les règles qui encadrent la sortie du trafic au-delà du réseau de l'utilisateur, comme les règles de blocage ou de filtrage)¹¹⁹³. La

¹¹⁹⁰ MEROLA A., « Utilisation et abus sur le protocole ICMP », préc., *Hakin9*, 2006, p. 50

¹¹⁹¹ Anssi, « Recommandations de configuration d'un système GNU/Linux », 22 fév. 2019, p. 22 ; « Limitations de routeur VRRP de couche 2 et 3 », sur *Docs.oracle.com*, consulté le 17 juil. 2023

¹¹⁹² « PF – Traffic Redirection (Port Forwarding) », préc., sur *Openbsd.org*, consulté le 17 juil. 2023

¹¹⁹³ On rappelle que le NAT redirige le trafic sortant d'un réseau interne vers le destinataire situé au-delà de ce réseau, tandis que la redirection de ports redirige le trafic entrant dans un réseau interne vers une machine destinataire membre de ce réseau. Les VPN ici étudiés utilisent seulement la redirection de ports pour communiquer les informations, sans utiliser le NAT. Par conséquent, les règles qui limitent le trafic sortant (à destination de tel ou tel réseau/machine/site web/page web...) ne

redirection de ports est dans ce cas utilisée entre autres pour faciliter le contournement des règles de blocage et de filtrage appliquées par les opérateurs. En d'autres termes, la redirection de ports est notamment exploitable pour réduire l'efficacité des règles étatiques et privées de blocage et de filtrage.

Autre exemple : durant les années 2000 et début 2010, l'opérateur Free bridait l'accès à tous les ports supérieurs au port 1023 afin de prioriser la bande passante accordée au trafic Web et mail¹¹⁹⁴. La redirection de ports peut dans ce cas être très utile pour contourner la restriction de Free. Supposons qu'une utilisatrice, Alice, veuille accéder à World of Warcraft (WoW), un jeu vidéo très populaire dans les années 2000 qui était accessible principalement sur les ports 1119, 3724 et 6012. Pour contourner cette restriction, il suffit à Alice de connaître l'adresse IP de la passerelle d'un ami abonné chez un FAI concurrent, puis de configurer la table de routage de son propre terminal pour que les paquets destinés aux serveurs de WoW sur les ports 1119, 3724 et 6012 soient adressés à la passerelle concurrente sur un port non bridé par Free (par ex. port 81). De cette façon, les paquets destinés à WoW seront transmis par la passerelle de Free à la passerelle concurrente sur le port 81 et, en lisant la destination des paquets, la passerelle concurrente redirigera les paquets vers les ports 1119, 3724 ou 6012. Comme la redirection ICMP, la redirection de port a pour effet de modifier l'adresse IP source. Les serveurs de WoW ne liront donc pas l'adresse IP d'Alice, mais celle de son ami dont la passerelle redirige le trafic.

Enfin, la redirection vers une A-DATA n'est pas seulement exploitée pour contourner une technique de restriction, mais ladite redirection peut elle-même être contournée ou délaissée. On reprend l'exemple des redirections DNS, grâce auxquelles les visiteurs de pages web à caractère terroriste ou pédopornographiques sont redirigés vers une page d'information du ministère de l'intérieur. Certes, les pages terroristes/pédopornographiques (R-DATA) redirigées renvoient vers une A-DATA, mais d'autres pages terroristes/pédopornographiques peuvent apparaître sur internet et peuvent être accédées par les utilisateurs. Les internautes désireux d'accéder à ces pages abandonneront celles qui redirigent vers la page ministérielle, et se rendront sur des pages équivalentes non identifiées par l'administration. En agissant ainsi, ils délaissent la A-DATA (page ministérielle) vers laquelle redirigent les pages bloquées, et

s'appliquent pas en l'espèce. PureVPN est l'un des rares services VPN reposant sur la redirection de ports. Sur le fonctionnement d'un VPN par redirection de ports, v. « Comment configurer la redirection de port et éviter le CGNAT », sur *Purevpn.fr*, 3 oct. 2022 ; et « Redirection de port et VPN : quel intérêt et comment ça fonctionne ? », sur *Frandroid.com*, 3 oct. 2021

¹¹⁹⁴ « Tutoriel : Contourner le bridage de ports de certains FAI », *Archives du site du zéro* [sdz.tdct.org], consulté le 19 juil. 2023. Le Site du Zéro était un site web de référence pour la qualité et le professionnalisme de ses tutoriels informatiques (notamment pour l'apprentissage des langages de programmation). Rebaptisé OpenClassrooms en 2013, il propose depuis 2015 des formations diplômantes reconnues par l'État. Concernant les nombreux témoignages des utilisateurs de Free sur le bridage de leurs ports, v. entre autres : « Attention à Free qui bride les ports », sujet de discussion publié par Eric [pseudonyme], sur le forum *Generation-nt.com*, 1^{er} déc. 2005 ; « Liste des ports bridés/non-bridés », sujet de discussion publié par flyco [pseudonyme], sur le forum *Freenews.fr*, 21 déc. 2005 ; « Ports bloqués chez free ? – obliger de changer les ports de ma mule », sujet de discussion publié par buzzleclair [pseudonyme], sur le forum de *Clubic.com*, janv. 2006 ; « Free bride ma connexion », sujet de discussion publié par Darkhopes [pseudonyme], sur le forum de *Commentcamarche.net*, 17 mars 2008 ; « Port 6881 restreint par Free et interdit accès à des sites », sujet de discussion publié par didier666 [pseudonyme], sur le forum de *Universfreebox.com*, 10 fév. 2009 ; « Free bride mes ports », sujet de discussion publié par codex42 [pseudonyme], sur le forum de *Freenews.fr*, 30 mars 2012

contournent la redirection et le blocage en migrant vers d'autres pages terroristes/pédopornographiques. Le blocage par redirection vers une A-DATA sera alors délaissé et contourné. Examinons la configuration suivante : supposons que 100 internautes français consultent des contenus terroristes ou pédopornographiques ; parmi ces 100 internautes, 90 sont fortement attachés à cette consultation ; le blocage par redirection mis en œuvre risque dans ce cas d'être contourné par 90 internautes. La R-DATA « consultation de contenus terroristes ou pédopornographiques » conservera alors la quasi-totalité de son échelle de diffusion (90 internautes au lieu de 100) malgré le blocage par redirection vers une A-DATA. En d'autres termes, la redirection d'une R-DATA vers une A-DATA n'empêche pas la reproduction de cette R-DATA sur internet, ne garantit pas durablement une large diffusion de la A-DATA (page ministérielle), et ne réduit que relativement l'échelle de diffusion d'une R-DATA si le risque de contournement est élevé. En somme, la redirection vers une A-DATA a pour inconvénients de faciliter les cyberattaques, d'être exploitable pour contourner les techniques de restriction, et d'être elle-même très vulnérable aux contournements.

C) La redirection de l'accès vers une A-DATA depuis le stockage de données

Lorsque la **redirection vers une A-DATA est pratiquée depuis un hôte** (machine de stockage), elle permet d'**agir sur les requêtes exécutées par cet hôte et les contenus qu'il héberge individuellement**, plus précisément que le ferait une redirection pratiquée depuis un routeur. *A contrario*, la **redirection vers une A-DATA pratiquée depuis un routeur** est plus appropriée pour **agir sur le trafic général** circulant dans un réseau national. Malgré cette différence importante, on observe que les avantages et inconvénients relevés pour la redirection dès la transmission valent également pour la redirection dès le stockage.

Premier avantage : la redirection d'une R-DATA vers une A-DATA dès le stockage contribue au bon fonctionnement du réseau. Par exemple, les redirections de port peuvent être mises en œuvre dès l'hôte (terminal ou serveur) et pas seulement dès le routeur. Typiquement, de nombreuses applications en ligne (principalement des jeux vidéo mais aussi certains VPN, certaines messageries instantanées...) ne sont accessibles que sur un ou plusieurs ports déterminés, et nécessitent que l'utilisateur effectue lui-même une redirection de ports depuis son terminal pour accéder à ces applications. La redirection de ports pratiquée dès le terminal permet dans ce cas à l'utilisateur d'accéder auxdites applications, et participe en ce sens au bon fonctionnement du réseau.

De même, les redirections URL mises en œuvre depuis un serveur permettent d'adapter l'itinéraire d'accès à ce serveur conformément aux modifications des adresses URL. En effet, il est d'usage fréquent que l'administrateur d'un site web redirige l'une de ses adresses URL vers une autre. Il peut ainsi rediriger définitivement une adresse URL1 vers une adresse URL2, auquel cas l'URL2 devient définitivement la page web vers laquelle renvoie l'accès à l'URL1. À cette fin, l'administrateur peut recourir à une redirection 301 (ou à une redirection 308, similaire). Cette méthode consiste à intégrer, dans une page web (URL1), un code logiciel dit « code 301 » indiquant au navigateur que cette page a changé d'adresse URL de façon permanente (au profit de l'URL2). L'administrateur peut utiliser la redirection 301 : pour que le trafic destiné à son ancien nom de domaine soit réacheminé vers son nouveau nom de domaine ; pour que le trafic destiné à l'ancien protocole d'accès à son nom de domaine (France) soit réacheminé vers son nouveau protocole d'accès (HTTPS) ; pour que le trafic destiné à certaines pages d'un site web soit réacheminé vers d'autres pages du même site qui comportent des contenus similaires ou

identiques (afin de diminuer le problème de contenus dupliqués) ; pour que le trafic destiné à la page d'un site web soit réacheminé vers une autre page qui fusionne les deux sur le même site... En somme, la redirection 301 permet aux administrateurs de sites web d'adapter l'itinéraire du trafic aux changements de noms de domaine, aux passages au protocole sécurisé HTTPS, aux fusions de pages et de sites web etc.

L'administrateur du site peut aussi rediriger *provisoirement* une adresse URL (URL1) vers une autre (URL2), auquel cas l'URL2 devient temporairement la page web vers laquelle renvoie l'accès à l'URL1. Il possède deux principaux outils à cette fin : les redirections 302 et 307. Les différences entre ces deux types de redirection est d'abord historico-technique ¹¹⁹⁵. Leurs différences résident ensuite dans les usages : les moteurs de recherche référencent les pages web qui contiennent un code 302, mais ne semblent pas référencer les pages qui contiennent un code 307¹¹⁹⁶. La redirection 302 devient alors un enjeu pour optimiser le référencement d'une page web par un moteur de recherche, et la redirection 307 est moins adoptée en raison de sa réputation de non-référencement. La redirection provisoire peut servir plusieurs fins : tester une fonctionnalité d'une page web et/ou la conception de cette page, rediriger l'utilisateur vers une offre promotionnelle (pop-up...), vers la bonne version d'une page selon les paramètres linguistiques de l'utilisateur, vers une page d'attente lorsque le site est en maintenance etc.

L'administrateur d'un logiciel client peut aussi pratiquer des redirections dès le terminal. On rappelle qu'un « client » est le logiciel local (présent sur le terminal) qui communique avec les serveurs – un navigateur web (client web), une application VPN (client VPN), une application mobile qui utilise une connexion internet, un jeu vidéo installé sur le terminal qui utilise une connexion internet... Deux principaux outils de redirection sont à disposition de l'administrateur d'un navigateur web : la redirection JavaScript ; et la redirection Meta refresh. La redirection JavaScript indique au navigateur qu'il doit immédiatement charger une autre adresse URL ; la redirection Meta refresh indique au navigateur qu'il doit rafraîchir la page ou rediriger l'utilisateur vers une autre URL après un délai de chargement. La redirection Meta refresh est particulièrement utile pour que le navigateur redirige la requête d'un utilisateur vers la page web d'un moyen de paiement en ligne à l'issue d'une commande passée par l'utilisateur.

¹¹⁹⁵ Aux débuts du Web, certains sites web utilisaient la méthode GET pour accéder aux URL – auquel cas les données à transmettre au serveur sont écrites directement dans l'URL (par ex. [www.exemple.com/register.php?firstname=olivier&name=berlin&age=30&gender=ma le](http://www.exemple.com/register.php?firstname=olivier&name=berlin&age=30&gender=male)). Désormais, la plupart des sites web utilisent la méthode POST – auquel cas les paramètres de l'URL (firstname, name, age, gender...) ne sont pas écrits dans l'URL mais dans la requête HTTP destinée au serveur. V. « GET et POST : comparaison des deux principales requêtes HTTP » [en ligne], *Ionos*, 11 août 2020. La redirection 302 permet d'accéder à une adresse URL en suivant la méthode GET ; la redirection 307 permet d'accéder à une adresse URL en suivant uniquement la méthode POST. Dans les faits, les administrateurs de sites web et les navigateurs web peuvent aussi bien exploiter la redirection 302 que la redirection 307 pour n'importe quelle page web : si une URL obéissant à la méthode GET (en principe redirection 302) exploite une redirection 307, les paramètres de l'URL ne seront tout simplement pas mentionnés dans le navigateur. La différence entre les redirections 301 et 308 suit la même logique. La redirection 301 rend possible l'accès à une URL selon la méthode GET, tandis que la redirection 308 rend possible l'accès à une URL exclusivement selon la méthode POST. Les différences entre les types de redirections HTTP et leurs raisons d'être historiques sont résumées par la section 6.4 de la RFC 7231 de juin 2014. V. aussi « 307 Temporary Redirect », *Developer.mozilla.org*, mäj le 20 juil. 2023

¹¹⁹⁶ AMICI Olivier, « Guide ultime des redirections : tout ce que vous devez savoir sur la redirection d'URL » [en ligne], *Semrush*, 11 fév. 2021

Concrètement, la page web redirigée intègre un code qui indique au navigateur l'URL de redirection ; et en retour, le navigateur intègre une redirection Meta refresh pour renvoyer le trafic vers l'URL de redirection. Les redirections tant JavaScript que Meta refresh sont pratiquées dès le terminal, ce qui implique que les pages redirigées ne peuvent pas être référencées par un moteur de recherche contrairement aux redirection France (301, 302, 307, 308...). De telles redirections sont donc déconseillées si l'administrateur du site désire optimiser le classement de sa page par un moteur de recherche.

En somme, les redirections URL pratiquées dès l'hôte offrent des capacités basiques comme la possibilité pour l'utilisateur de payer une commande passée sur un site marchand, l'accès à un nom de domaine qui a changé, la fusion de pages web voire de noms de domaines, le passage du protocole d'accès France au protocole sécurisé HTTPS, les tests pratiqués sur la conception et les fonctionnalités d'une page web, le renvoi vers une page d'attente lorsque le site est en maintenance... Les redirections URL permettent ainsi d'adapter l'itinéraire du trafic sur le réseau aux évolutions des adresses URL et à leurs interactions. En adaptant l'itinéraire du trafic au paysage URL d'internet, les redirections URL dès l'hôte participent au bon fonctionnement du réseau, tout comme celles pratiquées dès le routeur.

Deuxième avantage de la redirection d'une R-DATA vers une A-DATA dès l'hôte : **la redirection vers une A-DATA convertit l'accès à une R-DATA en un accès à une A-DATA.** Pour donner des exemples de redirections d'une R-DATA vers une A-DATA depuis l'hôte (terminal ou serveur), on a vu que l'application TikTok en fait usage pour que les requêtes d'accès destinés aux contenus relatifs à l'automutilation et au suicide soient réacheminés vers la page d'un service d'aide aux victimes. L'accès à la R-DATA « contenus à caractère automutilateur et suicidaire » est ainsi converti en un accès à la A-DATA « service d'aide aux victimes ». Que la redirection vers une A-DATA soit pratiquée depuis un terminal ou un serveur, on observe donc les mêmes avantages que ceux déjà rapportés pour la redirection pratiquée depuis un routeur.

Il en va de même pour les inconvénients. Premier inconvénient de la redirection vers une A-DATA depuis un hôte : **les redirections vers une A-DATA facilitent de nombreux troubles à la sécurité du réseau.** On a vu que l'existence même d'une redirection donne le pouvoir, à quiconque la contrôle, de réacheminer le trafic n'importe où sur internet. Il suffit alors au cyberattaquant de trouver le moyen de contrôler cette redirection pour détourner une vaste part du trafic. Les attaques par redirection ICMP sont praticables aussi bien depuis un routeur que depuis un serveur ou un terminal.

De même, les redirections DNS (redirections d'URL, d'adresses IP, de noms d'hôte...) donnent la possibilité de mener des attaques par redirection DNS. Par exemple, la passerelle (box, modem...) fournie par le FAI comporte un résolveur DNS qui fonctionne comme un serveur de cache : le résolveur stocke brièvement les requêtes DNS (les « met en cache ») de sorte que, si l'utilisateur souhaite accéder à un site web très récemment consulté, il peut le faire directement en accédant au cache de son résolveur, sans devoir traverser à nouveau l'ensemble du réseau DNS (serveurs de registrars, registries et racines). Le cyberattaquant peut ainsi exploiter une vulnérabilité d'un serveur DNS pour intégrer dans son cache des entrées erronées. Profitant des redirections DNS, le cyberattaquant peut alors attaquer le résolveur auquel est connecté le serveur hébergeant [Google.com](https://www.google.com) par exemple, puis réacheminer le trafic vers un site compromis ou vers sa propre machine. Tous les utilisateurs accédant à [Google.com](https://www.google.com) seront alors redirigés vers ce site ou cette

machine tant que l'erreur n'est pas corrigée dans le cache – ou du moins tant qu'elle n'est pas identifiée¹¹⁹⁷. On parle dans ce cas d'attaque par empoisonnement de cache DNS. Une fois le cache DNS corrompu, l'attaquant peut en effet : réacheminer les données personnelles des utilisateurs (identifiants, messages privés, codes de carte bleu...) vers la machine du cyberattaquant ; rediriger les internautes vers une page web corrompue (pharming) soit pour provoquer le téléchargement d'un malware par l'utilisateur qui visite cette page (attaque par téléchargement furtif) soit pour conduire l'utilisateur à divulguer ses données personnelles sur une page web quasiment identique à la page attaquée (attaque par hameçonnage) ; rediriger les internautes vers un site web quasiment identique pour tromper ou voler la clientèle du site attaqué en se faisant passer pour ce dernier (attaque par usurpation DNS, ou *DNS spoofing*)... Outre les attaques par empoisonnement de cache DNS, l'attaquant peut – sans cibler le résolveur DNS – directement attaquer un routeur, un serveur ou un terminal afin de rediriger le trafic. On parle dans ce cas d'attaque par détournement DNS (*DNS hijacking*).

Par ailleurs, il n'est pas nécessaire de contrôler une redirection DNS pour l'utiliser dans le cadre de cyberattaques. En effet, de nombreuses redirections DNS créent des espaces réservés à certains utilisateurs, sans que ces redirections représentent en elles-mêmes des barrières solides face aux attaques. Par exemple, l'utilisateur inscrit sur un réseau social ou sur le site d'une revue scientifique (*i.e.* qui y possède un compte) peut accéder à certaines pages auxquelles ne peuvent pas accéder les visiteurs non-inscrits (*i.e.* qui n'y possèdent pas de compte). Ceci est permis par les redirections DNS, qui redirigent la page confirmant l'authentification de l'utilisateur vers les pages réservés aux utilisateurs inscrits. L'attaquant peut alors accéder à ces pages réservées en ignorant la redirection, de façon que son accès à ces pages n'est pas conditionné par une quelconque authentification. Lorsqu'une attaque repose sur le fait d'ignorer une redirection DNS, on parle d'attaque par EAR (*Execution After Redirect*)¹¹⁹⁸. Les attaques par EAR offrent ainsi à l'attaquant l'accès à de nombreuses données personnelles, en principe inaccessibles sans les identifiants de l'utilisateur. En étant contrôlables, ou en donnant l'accès à des espaces réservés, les redirections vers une A-DATA fragilisent ainsi la sécurité du réseau.

Deuxième inconvénient : **les redirections d'une R-DATA vers une A-DATA pratiquées dès l'hôte démultiplient les possibilités de contournement**. D'une part, les redirections vers une A-DATA peuvent elles-mêmes être contournées ou délaissées. On reprend l'exemple de TikTok, qui redirige les contenus à caractère automutilateur et suicidaire vers une page d'aide aux victimes. Ce blocage par redirection a été largement contourné par les utilisateurs du réseau social : les contenus portant les caractères « mort » et « dépression » renvoyant vers la page d'aide aux victimes, les utilisateurs ont partagé leurs contenus traitant de ces sujets en employant les caractères « unalive » et « depre\$\$ion »¹¹⁹⁹. L'utilisation du blocage aggrave par ailleurs le risque de sur-blocage comme on l'a déjà relevé, donc aggrave le risque que soient bloqués les contenus d'utilisateurs n'incitant ni au suicide ni à l'automutilation (utilisateurs

¹¹⁹⁷ On a vu que Google.com est hébergé sur plusieurs serveurs DNS, dans le but de décentraliser le fonctionnement de son réseau DNS et de le sécuriser contre les attaques. Une fois l'attaque identifiée, le serveur attaqué pourra donc se rendre indisponible puis rediriger le trafic vers un autre serveur hébergeant Google.com, qui prendra alors le relai des requêtes DNS destinées à Google.com.

¹¹⁹⁸ PAYET Pierre, DOUPÉ Adam, KRUEGEL Christopher et VIGNA Giovanni, « EARs in the Wild : Large-Scale Analysis of Execution After Redirect Vulnerabilities », *SAC '13: Proceedings of the 28th Annual ACM Symposium on Applied Computing*, mars 2013, p. 1792-1799

¹¹⁹⁹ PROTAIS Marine, « "Algospeak" : les tiktoeurs contournent les algorithmes en inventant un nouveau langage », *L'ADN*, 13 avr. 2022

publiant leurs expériences et conseils après être sortis de la dépression, utilisateurs décrivant les causes et traitements de la dépression...), dont aggrave le risque ces utilisateurs sur-bloqués contournent à leur tour le blocage. En l'espèce, les redirections vers une A-DATA semblent largement contournées et délaissées par les utilisateurs.

D'autre part, les redirections vers une A-DATA offrent aux utilisateurs des outils de contournement. Avec l'exemple du bridage de ports par Free contourné grâce à la redirection de ports, on a constaté que **les redirections vers une A-DATA** (en l'espèce les redirections de port, qui permettent à l'utilisateur d'accéder depuis le réseau public à un serveur hébergeant une application) **sont exploitables pour contourner une A-DATA promue par le régulateur** (ports priorisés par Free) **et accéder à une R-DATA** (libre accès aux ports bridés par Free). Il en va de même pour la redirection DNS. On a vu qu'une redirection DNS permet de réacheminer l'utilisateur vers des pages web admises par le régulateur (accès de l'utilisateur à son compte utilisateur, accès de l'utilisateur à un site web qui a changé de nom de domaine, accès de l'utilisateur à un site web qui est passé au protocole sécurisé HTTPS, accès de l'utilisateur à des fonctionnalités testées par l'administrateur du site web...). Les redirections DNS sont pourtant facilement exploitables pour contourner une A-DATA promue par le régulateur et accéder à une R-DATA. Reprenons l'exemple du blocage par redirection des sites pédopornographiques et terroristes vers la page d'information du ministère de l'intérieur. Ce blocage effectué par les FAI peut être contournée à l'aide de la redirection DNS. Il suffit à l'utilisateur d'accéder aux paramètres de son système d'exploitation, puis de remplacer l'adresse IP du résolveur DNS de son FAI par les adresses IP d'un résolveur DNS alternatif (Google, CloudFlare, VeriSign, OpenDNS...) ¹²⁰⁰. De cette façon, l'utilisateur pourra accéder aux pages litigieuses sans se voir redirigé vers une page du ministère de l'intérieur.

Paragraphe 3 – Techniques basées sur les services et les contenus pour augmenter spécifiquement l'accès à une A-DATA

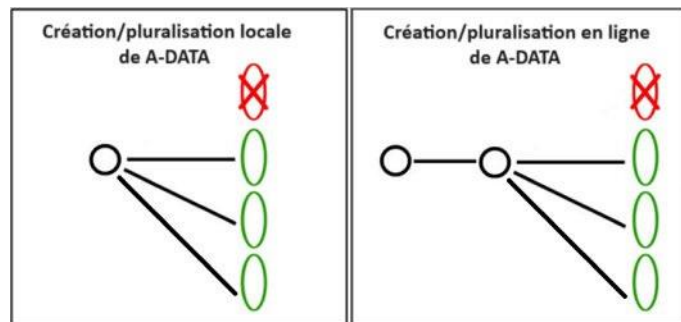
Parmi les techniques d'augmentation de l'accès qui ciblent des A-DATA, on s'intéressera longuement à la technique de création et/ou de pluralisation de A-DATA, que ces A-DATA soient des services (A) ou des contenus (B). On en déduira les avantages et inconvénients de cette technique (C) avant d'explorer deux autres techniques d'augmentation qui ciblent des A-DATA et reposent sur les services et contenus : la surexposition et la réutilisabilité de A-DATA (D).

¹²⁰⁰ ABALLEA Arthur, « Comment contourner un blocage DNS », *Blogdumoderateur.com*, 24 juin 2022

A) La création et/ou la pluralisation des services admis par le régulateur : l'exemple de la Chine

1. La stratégie technologique chinoise

On appelle « création et/ou pluralisation d'une A-DATA » la technique qui consiste, pour le régulateur, à provoquer la création ou la démultiplication du nombre de A-DATA sur internet. Comme l'accélération discriminée de l'accès à une A-DATA ou la redirection vers une A-DATA, la pluralisation d'une A-DATA vise à promouvoir une donnée admise par le régulateur.



La décentralisation participe à la pluralisation, mais les deux ne se confondent pas. Tandis que la décentralisation consiste à diversifier les voies d'accès à des données, la pluralisation consiste à augmenter la quantité de données accessibles. Par conséquent, il est tout à fait possible de pluraliser des A-DATA dans un système centralisé : un service central (par ex. Google Search) peut très bien à lui seul pluraliser l'accès à un grand nombre de A-DATA sur son service.

Dans l'Union européenne, on a déjà rapporté que plusieurs initiatives publiques ont soutenu voire créé des services en ligne (la boîte de messagerie allemande De-Mail, le moteur de recherche français Qwant, le moyen de paiement « Initiative Européenne de Paiements », le fournisseur cloud européen Gaia-X...) pour proposer une alternative européenne aux services en ligne américains (Gmail, Outlook, Google, Bing, Paypal, Apple Pay, Google Cloud Service, Amazon Web Service...). L'UE et certains de ses États membres sont ici intervenus pour augmenter le nombre de services en ligne légalement accessibles. Ce faisant, ils ont pluralisé l'offre de services admis par les régulateurs.

En Chine, la promotion et la démultiplication des services numériques nationaux sont le fruit d'un fort interventionnisme étatique. On a vu que l'État ordonne le blocage et le filtrage de nombreux services étrangers depuis les années 2000. Ce vaste système de restriction de l'accès est à double tranchant. D'un côté, il laisse aux entreprises chinoises un grand espace pour se développer sur le marché numérique chinois, sans subir la concurrence étrangère. D'un autre côté, le fait d'empêcher l'accès à de très nombreux services aggrave le risque de contournement (*i.e.* le nombre de personnes qui peuvent trouver un intérêt à contourner les restrictions), comme on le détaillera plus loin¹²⁰¹. En effet, une restriction excessive de l'offre (services accessibles) peut frustrer la demande (utilisateurs), ne pas couvrir toute la diversité d'intérêts individuels qui composent cette demande, et ainsi conduire certains utilisateurs frustrés à se tourner vers une offre alternative satisfaisant davantage leurs intérêts individuels que l'offre légale. En d'autres termes, le risque de contournement peut être limité si l'offre légale satisfait

¹²⁰¹ Précisons au moins que, par définition, le contournement d'une restriction est une réaction à ladite restriction. L'existence même d'une restriction donne donc naissance au risque de contournement. Plus la restriction est intense, plus le risque de contournement est élevé dans l'absolu (*i.e.* hors de toute autre circonstance et technique de régulation employée). Ce risque absolu peut néanmoins être largement relativisé ou atténué grâce à plusieurs techniques de régulation.

la diversité de la demande¹²⁰². En l'espèce, cela signifie que si les entreprises chinoises satisfont la diversité de la demande nationale, alors sera limité le risque que la population chinoise contourne les restrictions pour accéder aux services étrangers bloqués/filtrés.

Lorsqu'un régulateur restreint massivement l'accès aux services étrangers, l'enjeu consiste donc à maximiser les avantages de cette restriction (priorisation des entreprises nationales) tout en minimisant les inconvénients (aggravation du risque de contournement, qui peut être largement minimisé si la demande nationale est satisfaite par l'offre nationale). On ignore si la Chine a précisément envisagé qu'une satisfaction de la demande nationale par l'offre nationale minimiserait les inconvénients de la restriction des services étrangers. Il n'en reste pas moins que l'Empire du Milieu semble avoir limité ces inconvénients en visant une certaine autosuffisance économico-numérique.

Le fait que la Chine ait aujourd'hui ses propres géants du numérique n'était pas une réalité qui allait de soi dans les années 1990, ni même 2000. Au début des années 1980, l'économie numérique chinoise repose sur deux types d'acteurs : de grandes entreprises (Legend, Founder...) qui, issues d'universités et d'instituts de recherche chinois, bénéficient des résultats de la recherche scientifique et sont ainsi en position de rivaliser avec les firmes multinationales ; et des entreprises industrielles qui produisent massivement des équipements en technologie d'information et de la communication (TIC)¹²⁰³. Cette séparation de la recherche et de l'industrie n'a pas fonctionné, et a ralenti la croissance technologique chinoise. Les cloisons entre le milieu universitaire et le milieu entrepreneurial étaient si fortes que les industries chinoises ont peu intégré les progrès technologiques universitaires¹²⁰⁴. Par ailleurs, les industries chinoises étaient spécialisées dans des domaines faiblement créateurs de valeur ajoutée – à savoir l'assemblage de produits importés. Les industries n'ont alors pas pu faire preuve d'innovation, et ont joué sur l'amélioration de la production quantitative (brevets utilitaires et de conception) plutôt que sur la qualité des produits (brevets de technologies essentielles). Le volume d'équipements TIC produits industriellement, combiné au faible coût de la main d'œuvre, ont permis aux industries chinoises de vendre un très grand nombre de produits à bas prix. En 2005, la Chine dépasse les États-Unis pour devenir le premier exportateur mondial d'équipements TIC¹²⁰⁵.

Ce modèle économique qui repose sur l'assemblage et les exportations montre rapidement ses limites : par définition, l'assemblage de produits importés dépend des produits importés, donc la source de revenus des industries chinoises (exportations) dépend très largement des entreprises étrangères ; par ailleurs, les industries chinoises ne parviennent pas à créer de la valeur ajoutée pour les raisons exposées, et les profits générés par le produit transformé reviennent alors principalement aux entreprises étrangères innovantes qui vendent leurs produits assemblés en Chine ; de plus, si les produits sont certes assemblés par les industries

¹²⁰² On a vu que d'autres techniques de régulation peuvent contribuer à réduire le risque de contournement – la centralisation, le chiffrement, la modération par IA...

¹²⁰³ CAO Cong, « L'industrie chinoise face au défi technologique », *Perspectives chinoises*, n° 83, mai-juin 2004

¹²⁰⁴ *Ibid.* : « peu d'entreprises chinoises possèdent des droits de propriété intellectuelle sur les technologies essentielles (...). Les entreprises chinoises semblent être plus intéressées par les brevets utilitaires et les brevets de conception qui n'apportent pas de modification substantielle »

¹²⁰⁵ SACHWALD Frédéric, « La Chine, puissance technologique émergente », *Institut français des relations internationales (IFRI)*, juin 2007, p. 4

chinoises, ils sont principalement exportés par des entreprises à capitaux étrangers (partiellement ou totalement), et les exportations chinoises dépendent donc des investissements étrangers¹²⁰⁶.

Pour sortir de la dépendance aux entreprises et investissements étrangers, la Chine adopte une stratégie asiatique aussi choisie par le Japon, la Corée du Sud et Taiwan : assimiler les technologies importées, et leur apporter une valeur ajoutée pour pouvoir innover et créer des sources nationales de richesse. Cette stratégie s'appuie sur le concept de « transferts de technologies », *i.e.* l'étude des technologies importées dans le but d'inspirer la fabrication de variantes nationales porteuses de valeur ajoutée. Ainsi, « *les firmes coréennes sont progressivement passées de la production de produits conçus à l'étranger (Original Equipment Manufacturing – OEM) à la fabrication de produits conçus en Corée (Own Design Manufacturing – ODM) et à celle de leurs propres marques (Own Brand Manufacturing – OBM)* »¹²⁰⁷. Pour récupérer de la valeur ajoutée, tous ces pays investissent dans la recherche scientifique synchronisée avec la production industrielle.

En Chine, lors des Conférences nationales sur l'innovation technologique de 1997 et 1999, le gouvernement appelle d'abord les entreprises à investir dans la R&D (1997) puis à consacrer au moins 5% de leurs ventes annuelles à la R&D (1999)¹²⁰⁸. Entre 2000 et 2004, les investissements des entreprises en R&D bondissent, et la Chine devient en 2004 le troisième pays à investir le plus en R&D dans le monde¹²⁰⁹. L'investissement dans la R&D met du temps à porter ses fruits. Tant le Japon que Taiwan et la Corée du Sud ont connu un « *décalage entre importations technologiques et innovations nationales* », mais le décalage était encore très intense en Chine au milieu des années 2000¹²¹⁰. Les industries chinoises se sont spécialisées dans des exportations de produits faiblement créateurs de valeur ajoutée (équipements TIC), tandis que les industries sud-coréennes se sont spécialisées dans les exportations de produits fortement créateurs de valeur ajoutée (la haute technologie, *i.e.* les technologies les plus complexes et récentes sur un marché incluant la pharmacie, la robotique, l'aérospatiale...) ; les investissements dans la recherche fondamentale ont été légers en Chine, tandis qu'ils étaient conséquents en Corée du Sud¹²¹¹.

¹²⁰⁶ CAO C., « L'industrie chinoise face au défi technologique », préc., 2004 : « *en 2000, 92,5 % des systèmes informatiques et 96,4 % des équipements de télécommunications mobiles étaient exportés par des entreprises à capitaux étrangers* ». En 2002, « *le traitement et l'assemblage de matériaux en provenance de l'étranger représente quelque 90% des exportations chinoises de hautes technologies. (...) [Les industries chinoises] sont centrées sur des activités d'assemblage, sur des produits bas de gamme et à faible valeur ajoutée, et sont dominées par des entreprises à capitaux étrangers. Aussi la Chine fabrique-t-elle et exporte-t-elle de grandes quantités de produits high-tech sans pour autant créer la valeur ajoutée associée à ce genre de produits ; la majeure partie des profits va en effet aux propriétaires des technologies-clés.* »

¹²⁰⁷ *Ibid.*

¹²⁰⁸ *Ibid.*

¹²⁰⁹ SACHWALD F., « La Chine, puissance technologique émergente », préc., 2007, p. 11 : les dépenses de R&D chinoises représentaient 18% des dépenses américaines en 2000, contre 32,8% en 2004

¹²¹⁰ CAO C., « L'industrie chinoise face au défi technologique », préc., 2004

¹²¹¹ En 2005, la balance commerciale de la Chine est négative dans le domaine des hautes technologies : les industries de haute technologie représentaient -6,95% de la balance commerciale chinoise. La même année, les industries de haute technologie représentaient +5,1% de la balance commerciale sud-coréenne. Quant à l'investissement en recherche fondamentale, en 2002, 5,7% des dépenses chinoises en R&D étaient consacrées à la recherche fondamentale, contre 13,7% en Corée du

Autant de facteurs qui ont permis aux firmes sud-coréennes d'exporter des produits à forte valeur ajoutée et qui, au contraire, ont ralenti la création de valeur ajoutée en Chine. En 2004, alors que la Corée du Sud avait déjà ses propres marques compétitives sur le marché international (Samsung, LG Electronics, Hyundai, Naver...), « aucune des grandes entreprises d'État chinoises (...) n'est devenue un géant internationalement compétitif, avec un marché, une marque et un système d'achat international »¹²¹².

Pour accélérer la création de valeur ajoutée en Chine, le parti-État lance en 2006 le Plan national de développement des technologies et des sciences à moyen et long terme (2006-2020), par lequel il fixe cinq objectifs à atteindre d'ici 2020 : augmenter à 2,5% du PIB les dépenses de R&D ; élever à plus de 60% la part que représentent les progrès technologiques dans la croissance économique ; réduire à moins de 30% la dépendance de la Chine vis-à-vis des importations de technologies ; figurer parmi les cinq premiers pays par le nombre de brevets d'invention délivrés à ses citoyens ; et aboutir à ce que les articles scientifiques rédigés par des chercheurs chinois soient parmi les plus cités au monde. Afin d'atteindre ces objectifs, le ministère du Commerce invite en 2006 les industries chinoises à se spécialiser de plus en plus dans l'importation de haute technologie¹²¹³. En 2010, le même ministère définit en quatre étapes le processus à suivre par les industries chinoises pour produire de la valeur ajoutée sur les produits importés : l'introduction (*i.e.* l'importation d'une technologie étrangère), la digestion (inclusion de la technologie dans un processus de fabrication), l'absorption (intégration de la technologie dans la chaîne de production) et la ré-innovation (amélioration de la technologie importée)¹²¹⁴.

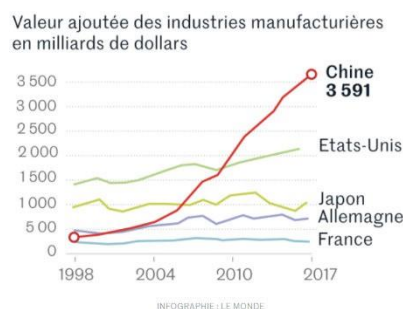
Sud et 18% aux États-Unis. V. SACHWALD F., « La Chine, puissance technologique émergente », préc., 2007, p. 10 et 12

¹²¹² CAO C., « L'industrie chinoise face au défi technologique », préc., 2004

¹²¹³ Ministère chinois du Commerce, Catalogue des technologies encouragées à être importées en Chine (中国鼓励引进技术目录) du 18 déc. 2006

¹²¹⁴ Ministère chinois du Commerce, Opinions directrices pour encourager la digestion, l'absorption et la ré-innovation des technologies importées (关于鼓励引进技术消化吸收再创新的指导意见) du 16 déc. 2010

Dès la moitié des années 2010, l'UNESCO estime que chacun des objectifs du Plan de 2006 a été quasiment atteint, mais constate toujours un « *décalage entre l'augmentation des intrants en matière de R&D et les résultats scientifiques et technologiques relativement modestes* »¹²¹⁵. Malgré une innovation décevante, les efforts régulateurs de la Chine ont très fortement stimulé la création de valeur ajoutée. Depuis 2010, la Chine est ainsi le pays dont les industries manufacturières produisent le plus de valeur ajoutée (schéma ci-contre)¹²¹⁶.



2. Le plan Made in China 2025

Le début des années 2010 marque aussi l'entrée des géants de l'internet chinois sur le marché international¹²¹⁷. En 2015, le plan *Made in China 2025* (MIC 2025) abandonne la stratégie quantitative d'exportations de produits bon marché, au profit d'une stratégie qualitative de production de biens et services innovants et hauts-de-gamme. Avec ce 13^e plan quinquennal, le gouvernement souhaite spécialiser les industries chinoises dans la haute technologie (voitures électriques, équipements d'énergie renouvelables, technologies maritimes, robotique, puces électroniques...), améliorer significativement les capacités d'innovation, augmenter significativement la productivité de tous les employés, et faire passer à un stade supérieur l'intégration de l'industrie et de l'informatique en Chine. Pour suivre ces quatre principes directeurs, le MIC 2025 investit la somme colossale de 2 160 milliards de dollars afin que les industries chinoises satisfassent 40% de la demande chinoise en composants de base d'ici 2020 (*i.e.* acquièrent 40% des parts du marché intérieur dans le domaine des composants de base), puis 70% de la demande intérieure en 2025¹²¹⁸.

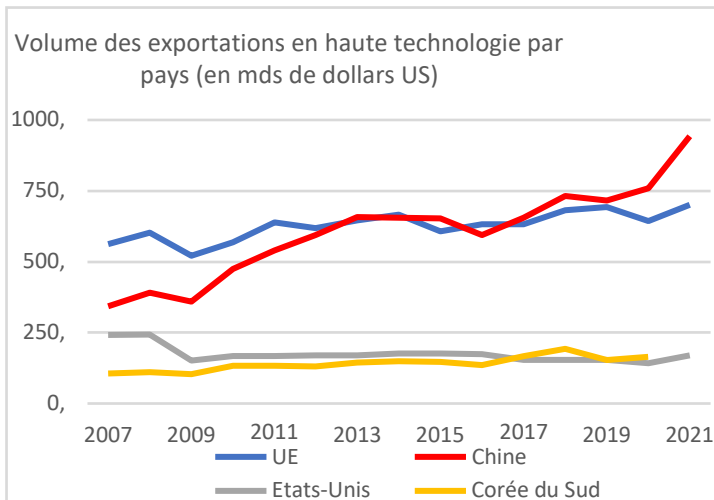
¹²¹⁵ CAO C., « Chine », in *Rapport de l'UNESCO sur la science : vers 2030*, 2016, p. 629. Sur la satisfaction de ces objectifs par la Chine, le rapport constate que « les [dépenses intérieures de recherche et développement] représentaient 2,09 % du PIB en 2014 [par rapport aux 2,5% prévus en 2020]. En outre, les progrès technologiques contribuent déjà à hauteur de plus de 50 % à la croissance économique [par rapport aux 60% prévus en 2020] : en 2013, les inventeurs chinois ont obtenu environ 143 000 brevets d'invention et la Chine s'est classée au quatrième rang mondial en nombre de citations d'articles scientifiques. D'après les prévisions, la dépendance de Pékin à l'égard de la technologie étrangère devrait baisser à environ 35 % en 2015. »

¹²¹⁶ Ce schéma est proposé par LEMAÎTRE Frédéric et LEPLÂTRE Simon, « Avec les nouvelles technologies Made China 2025, Pékin rêve d'autarcie », *Le Monde*, 27 janv. 2019

¹²¹⁷ En 2010, le groupe Alibaba donne naissance à l'application de commerce en ligne Aliexpress, version occidentale de Tao Bao. La même année est créée l'entreprise Xiaomi, aujourd'hui troisième plus important vendeur et exportateur de smartphones dans le monde et fabricant central en Chine de tablettes, objets connectés, écouteurs, manettes de jeu vidéo, trottinettes, télévisions intelligentes... En 2011, la messagerie instantanée WeChat est rendue publique par Tencent, et s'exporte assez bien (en 2013, sur les 300 millions d'utilisateurs actifs de WeChat, 60 millions ne résidaient pas en Chine).

¹²¹⁸ Dans le détail, d'ici 2025, les industries chinoises doivent fournir 80% du marché intérieur dans les secteurs des véhicules hybrides et électriques, des composants technologiques des navires et des équipements de production d'énergie renouvelable, 70% du marché intérieur dans les secteurs des robots industriels et des équipements médicaux de haute technologie, 60% dans le domaine des tracteurs et moissonneuses de haute technologie, 40% dans le secteur des puces pour smartphones, et 10% dans le secteur des avions gros-porteur. V. WÜBBEKE Jost, MEISSNER Mirjam, ZENGLEIN Max J., IVES Jacqueline et BJÖRN Conrad, *Made in China 2025. The making of a high-tech*

Le MIC 2025 a profondément crispé les relations géopolitiques et commerciales de la Chine avec les États-Unis et l'Europe, car le parti-État investit d'importants fonds publics pour réduire les parts de marché des industries étrangères qui ont fondé en Chine une composante parfois essentielle de leur modèle économique (Microsoft, Apple, IBM, Intel, Pfizer, AstraZeneca, Sanofi, Tesla, Volkswagen, ABB...) ¹²¹⁹. Au début des années 2020, la Chine semble en bonne voie pour atteindre certains de ces objectifs ¹²²⁰. Le MIC 2025 s'est accompagné d'une hausse effective des subventions à l'innovation, semble par ailleurs avoir eu un effet positif sur le ratio R&D/chiffre d'affaires en Chine et, depuis 2017, la Chine est devenue la première exportatrice mondiale de produits haute technologie ¹²²¹.



superpower and consequences for industrial countries, Mercator Institute for China Studies, 12 août 2016 ; LEMAÎTRE F. et LEPLÂTRE S., « Avec les nouvelles technologies Made China 2025, Pékin rêve d'autarcie », préc. *Le Monde*, 2019

¹²¹⁹ SCHAEFFER Frédéric, « Industrie : l'Europe s'inquiète des ambitions de la Chine », *Les Echos*, 8 mars 2017 ; LEPLÂTRE Simon, « Le plan "Made in China 2025" visé par les taxes américaines », *Le Monde*, 5 avr. 2018 ; DUGUA Pierre-Yves, « Après l'Europe, Trump déclenche la guerre commerciale avec la Chine », *Le Figaro*, 19 juin 2018

¹²²⁰ Concernant les équipements d'énergie renouvelable, la Chine a dépassé l'Europe pour devenir le pays le plus producteur d'énergie solaire depuis 2016, puis le pays le plus producteur d'énergie éolienne depuis 2020, puis le pays le plus compétitif par sa propriété industrielle dans les domaines de l'énergie éolienne et de la technologie solaire depuis 2021 (dépassant ainsi le Japon), et par ailleurs le pays le plus concentrateur des étapes de fabrication des panneaux solaires (en juillet 2022, 80% de toutes les étapes de fabrication des panneaux solaires étaient effectués en Chine d'après l'Agence internationale de l'énergie) : MAGUIRE Gavin, « Column: China widens renewable energy supply lead with wind power push », *Reuters*, 1^{er} mars 2023 ; TAKE Sayumi et IMAHASHI Rurika, « China drives global renewables spending to record 1st half », *Nikkei Asia*, 16 août 2022. Fin 2020, la capacité chinoise de production d'énergie renouvelable a même largement dépassé les objectifs gouvernementaux (396 GW pour l'hydroélectricité contre les 340 GW prévus, 282 GW pour l'éolien contre les 210 GW prévus, 253 GW pour le solaire contre les 110 GW prévus) : HOVE Anders, « Énergies renouvelables : le système d'innovation chinois peut-il favoriser la transition bas-carbone ? », *GREEN*, n° 1, 2021, p. 76-85. Concernant les voitures électriques, les 94 marques chinoises représentaient 81% du marché intérieur en 2022, et la Chine est devenue le pays le plus consommateur de voitures électriques au monde depuis 2015 (réduisant ainsi la dépendance de la Chine au pétrole étranger, limitant l'aggravation de la pollution atmosphérique, et donnant à l'industrie automobile chinoise la possibilité de concurrencer les industries automobiles européenne et américaine malgré le très important retard chinois sur la connaissance et l'innovation des moteurs à combustion) : CAMPBELL Peter, WHITE Edward, LI Gloria et NILSSON Patricia, « The Chinese carmakers planning to shake up the European market », *Financial Times*, 29 juin 2023 ; SCIULARA Auguste « La Chine est le leader mondial des voitures électriques : quels sont ses secrets ? », *Numerama*, 12 juil. 2023.

¹²²¹ BRANSTETTER Lee G., « Does "Made in China 2025" work for China ? Evidence from Chinese listed firms », *National Bureau of Economic Research*, nov. 2022, p. 13. Le schéma ci-contre s'appuie

Cependant, de nombreux objectifs n'ont pas été atteints, et l'Empire du Milieu reste très dépendant de l'économie étrangère : en 2020, les industries chinoises détenaient seulement 27% des parts du marché intérieur des robots industriels, un chiffre stable depuis 2015, loin des 50% espérés en 2020 par le MIC 2025 ; la même année, les industries chinoises détenaient 16% des parts du marché intérieur des puces électroniques contre les 40% prévus par le MIC 2025 (en grande partie à cause du retard technologique pris par la Chine dans le domaine) ; et le MIC 2025 ne semble pas avoir eu d'effet positif significatif (à un niveau de signification de 5%) sur les subventions totales, les brevets d'invention chinois, l'abandon des brevets utilitaires américains, la productivité du travail, ni même la marge bénéficiaire des entreprises chinoises¹²²².

Enfin, le gouvernement chinois s'est appuyé sur la coordination du système bancaire pour soutenir l'essor de grandes entreprises du numérique. En Chine, l'État est l'actionnaire majoritaire des neufs grandes banques du pays. La Banque populaire de Chine (banque centrale chinoise) « transmet aux banques commerciales des « instructions aux guichets » pour orienter les prêts en coordination avec la Commission nationale du développement et de la réforme, la Commission de régulation de la banque et de l'assurance et la Commission de régulation des marchés financiers »¹²²³. Huawei aurait ainsi obtenu des prêts et crédits de 41 milliards d'euros dans le cadre d'une « initiative conjointe pour financer le programme Made in China 2025 via le crédit bancaire et les marchés de capitaux » lancée par la Banque populaire de Chine en mars 2017. Les géants chinois Alibaba, Tencent, Baidu, Huawei ou encore Xiaomi ont ainsi bénéficié d'un système financier coordonné par l'État, qui privilégie les prêts accordés aux géants au détriment des petites entreprises¹²²⁴.

En somme, on identifie au moins cinq leviers économiques activés par le gouvernement chinois pour faire émerger technologiquement le pays : (i) la définition nationale de seuils minimaux d'investissement des entreprises dans la R&D et d'un processus de production créateur de valeur ajoutée, afin de stimuler l'innovation ; (ii) l'établissement de mesures

sur les données de la Banque mondiale (« Exportations de haute technologie (\$ US courants) » [en ligne]).

¹²²² Tandis que les parts de marché des industries chinoises stagnent en robotique depuis 2015, les industries chinoises sont de plus en plus demandeuses de robots industriels, comme l'illustre la forte hausse de la densité de robots (passant de moins de 15 robots pour 10 000 salariés en 2011 à 322 robots pour 10 000 salariés en 2021, dépassant la même année la densité de 274 robots pour 10 000 salariés aux États-Unis). Couplée à la stagnation des parts de marché des industries chinoises, la hausse de la demande chinoise en robotique fait dépendre de plus en plus de demandes aux industries étrangères. V. « China Aims for Global Leadership in Robotics with new 5-year Plan », *International Federation of Robotics*, janv. 2022 et « China: Robot installations grew by 44 percent », *International Federation of Robotics*, sept. 2022. Quant aux puces électroniques, Emily S. Weinstein, chercheuse au Center for Security and Emerging Technology de l'Université de Georgetown, souligne que « la Chine n'a pas (...) les "décennies, voire les siècles" d'expérience et de connaissances tacites nécessaires pour reproduire les machines de photolithographie ultraviolette extrême (EUV) nécessaires au développement de puces à 5 nm ou moins, ce qui constitue un obstacle critique pour la Chine dans la progression de ses puces vers les nœuds les plus avancés » : « Ask the Experts: Is China's Semiconductor Strategy Working? » [en ligne], *Blogs LSE* [London School of Economics], sept. 2022. Enfin, sur l'évaluation de l'efficacité économique du MIC 2025, v. BRANSTETTER L. G., « Does "Made in China 2025" work for China ? Evidence from Chinese listed firms », préc., *National Bureau of Economic Research*, 2022, p. 13

¹²²³ COELHO Ophélie, « Indépendance numérique : que nous apprend la Chine ? » [en ligne], *Institut Rousseau*, 30 nov. 2021

¹²²⁴ *Ibid.*

protectionnistes comme le plafonnement des investissements étrangers dans les secteurs technologiques les plus importants, ou l'attribution préférentielle de prêts et de subventions à des entreprises nationales plutôt qu'à des entreprises étrangères, afin de privilégier le développement économique des entreprises chinoises au détriment des entreprises étrangères et pour préserver la Chine contre les ingérences d'acteurs étrangers ; (iii) l'adoption d'une stratégie de transferts de technologies étrangères, pour améliorer leurs propres technologies nationales ; (iv) la spécialisation dans la production et l'exportation d'équipements de haute technologie, pour créer de la valeur ajoutée, générer du profit et s'intégrer dans l'économie mondiale ; et (v) la coordination du système bancaire, pour promouvoir l'essor national et international de géants technologiques chinois.

Parallèlement au blocage des applications en ligne étrangères, le gouvernement chinois a donc largement contribué à ce que l'offre technologique nationale se pluralise et couvre la diversité d'intérêts de la demande intérieure. Dès lors que les applications en ligne nationales satisfont la demande intérieure, l'État a largement réduit le risque que la population chinoise contourne les restrictions d'accès aux applications étrangères. Par exemple, WeChat qui était au départ une pâle copie de WhatsApp a rapidement prouvé sa valeur ajoutée par rapport à WhatsApp en devenant une application à tout faire¹²²⁵. De même, les applications de commerce en ligne fournissent des services extrêmement variés, dont des concepts qui n'existent pas en Occident – TaoBao (*design* chargé adapté aux attentes chinoises, première application de commerce en ligne à proposer la gratuité de la mise en vente de produits contrairement à Amazon qui prend une commission sur les ventes, à offrir une messagerie instantanée entre acheteurs et vendeurs, à fournir un double système de notation des vendeurs et des acheteurs, à donner aux vendeurs la possibilité de faire du streaming en direct pour promouvoir leurs produits...), Tmall (vente à bas prix de produits de marques), Pinduoduo (première application à concrétiser le modèle économique selon lequel plus il y a d'acheteurs d'un même produit, plus diminue le prix payé par chaque acheteur) etc. Les besoins de la demande intérieure sont vastement couverts par des applications chinoises dans la plupart des segments de marché, des moteurs de recherche (Baidu Search et Sogou respectivement détenus par Baidu et Tencent) aux services de vidéos à la demande (iQIYI et Tencent Vidéo, appartenant à Baidu et Tencent), en passant par les navigateurs web (QQ Browser, UC Browser, Opera...), la cartographie (Gaode Maps et Baidu Maps, appartenant à Alibaba et Baidu), les réseaux sociaux et messageries instantanées (WeChat, Douyin/TikTok, Toutiao, Weibo, Kuaishou, Bilibili, Little Red Book...), les moyens de paiement en ligne (Alipay, WeChat Pay, Union Pay, JD Pay, BestPay...), la distribution de musiques en streaming (KuGou, QQ Music, Kuwo appartenant tous à Tencent, NetEase Cloud Music appartenant à NetEase...), l'agrégation d'actualités (QQ News, Sina News...) , les encyclopédies en ligne (Baidu Baike, Baik.com...) ou encore les jeux vidéo en ligne (PUBG : Battleground, Honor of Kings, QQ Speed, League of Legends appartenant tous à Tencent, Onmyoji et Fantasy Westward Journey appartenant à NetEase...).

Les internautes chinois ont leurs habitudes d'usages, leurs contacts, leurs données voire leur métier sur ces diverses applications chinoises qui présentent d'importantes valeurs ajoutées par

¹²²⁵ Sur WeChat, il est possible pour l'utilisateur de rechercher d'autres utilisateurs par géolocalisation, de publier sur son profil des images et des textes courts de type microblog, de suivre l'actualité d'un utilisateur, possibilité de payer toute transaction avec WeChat Pay (factures de gaz, achats en boutiques...), de scanner des QR Code pour des démarches administratives (paiement d'impôts, procédure de divorce...), professionnelles, de réservation, de paiement, de communication privée avec certains contacts, et WeChat offre aussi aux créateurs d'applications en ligne (applications de réservation de taxis, de réservation d'hôtels, de livraison alimentaire, pages officielles d'entreprises...) d'intégrer leurs applis à WeChat à l'image d'un magasin d'applications

rapport aux applications étrangères. Sauf exception, ces internautes ont alors peu intérêt à contourner les blocages et filtrages pour utiliser des applications étrangères (WhatsApp, Facebook, Instagram, Snapchat, Twitter...) désertées par la population chinoise, inadaptées aux usages nationaux et dont les fonctionnalités sont déjà offertes voire améliorées par leurs applications nationales. Tel n'est pas le cas en Russie, où l'offre nationale ne suffit pas à couvrir les besoins de la demande nationale. On a vu ainsi que le blocage d'Instagram a été largement contourné faute d'une alternative nationale capable d'offrir les mêmes fonctionnalités et les mêmes outils de valorisation des contenus, entreprises et influenceurs. De même, le blocage de WhatsApp y est impossible sans risquer un contournement massif, faute d'une application nationale capable de supplanter la messagerie instantanée la plus utilisée en Russie.

À la différence de la Russie, la Chine a considérablement planifié et coordonné l'essor technologique national et la création de valeur ajoutée, en plus d'investir des sommes colossales dans le secteur. À la différence de l'UE, la Chine a restreint l'accès de sa population à la quasi-totalité des concurrents internationaux sérieux, et a instauré un protectionnisme économique qui rend le marché chinois difficile d'accès aux entreprises étrangères. **La Chine** a ainsi pu **maximiser les avantages du blocage et du filtrage** (prioriser les entreprises nationales) **tout en relativisant largement l'aggravation du risque de contournement** (grâce à la satisfaction de la diversité de la demande nationale par la pluralité et la qualité de l'offre nationale), et elle a pu **maximiser les avantages de la pluralisation de A-DATA** (satisfaire la diversité de la demande nationale par la pluralité de l'offre nationale légale) **tout en relativisant largement l'aggravation du risque de délaissement** des A-DATA par la population nationale (grâce à la création de valeur ajoutée par les applications en ligne chinoises). Combinée au blocage et au filtrage des applications étrangères, la pluralisation des A-DATA (en l'espèce, la diversification de l'offre nationale légale d'applications en ligne) a permis de contenir la population chinoise d'internautes dans un environnement de services en ligne quasi-exclusivement chinois¹²²⁶.

¹²²⁶ Précisons que la stratégie employée par la Chine pour satisfaire la demande intérieure par l'offre intérieure ne fonctionnera probablement pas pour tous les pays. En effet, la Chine a fait reposer sa stratégie technologique sur le très grand nombre de travailleurs au sein de la population chinoise (productions de masse, dont les profits des ventes et exportations ont permis de financer la R&D), et sur la présence de nombreuses terres rares en Chine (attractivité des industries et investissements étrangers, et production de puces de smartphones, d'écrans d'ordinateurs portables, d'équipements de production d'énergie renouvelable, de batteries de voitures électriques...). L'UE et les États-Unis auront donc des difficultés à concurrencer la Chine sur ces segments. En revanche, la productivité chinoise est particulièrement faible contrairement à l'UE et aux États-Unis. Or, la productivité des travailleurs est une source importante de création de valeur ajoutée, ce qui en fait un paramètre intéressant pour stimuler l'innovation occidentale, tout comme l'investissement dans la recherche fondamentale sur lequel la Chine a beaucoup de retard. Des stratégies axées sur les atouts économiques états-uniens et européens seront probablement plus adaptées pour que la pluralité de l'offre occidentale satisfasse la demande. Par ailleurs, le fait que la population chinoise soit intégrée dans un environnement de services en ligne quasi-exclusivement chinois n'empêche pas une forte dépendance de l'économie chinoise aux importations, aux entreprises et investissements étrangers comme on l'a vu, et ne doit pas non plus masquer le fait que la Chine accuse un retard difficilement rattrapable dans de nombreux domaines technologiques (puces électroniques, conception de systèmes d'exploitation, produits médicaux et pharmaceutiques...) dans lesquels les entreprises étrangères dominent très nettement les parts du marché intérieur chinois.

B) La pluralisation des contenus admis par le régulateur

Les services en ligne ne sont évidemment pas les seuls à pouvoir faire l'objet d'une pluralisation pilotée par l'État. L'État peut aussi stimuler une pluralisation des contenus admis par le régulateur. Depuis le début des années 2000, des administrations chinoises ont pris les unes après les autres des initiatives locales pour recruter des commentateurs en ligne payés pour diffuser la propagande du parti communiste chinois (PCC). Le Département de propagande du PCC de Changsha (capitale du Hunan) recrute officiellement les premiers propagandistes en ligne en 2004 ; l'Université de Nanjing embauche des étudiants depuis 2005 pour défendre l'action et les décisions du PCC contre les opinions défavorables au gouvernement ; la même année, les dirigeants du PCC du Jiangsu embauchent leurs premières équipes de commentateurs ; en 2007, était généralisé le recours à des équipes de commentateurs par les organes du PCC et les établissements d'enseignement supérieur¹²²⁷. En 2017, une étude scientifique évalue à 448 millions le nombre de messages propagandistes fabriqués par les autorités sur les réseaux sociaux chaque année¹²²⁸.

Surnommée péjorativement « Armée des 50 centimes » par les internautes chinois en raison de leur faible rémunération, les commentateurs propagandistes ne semblent pas convaincre la population, mais l'objectif de ces équipes ne réside probablement pas dans leur pouvoir de conviction. À défaut de susciter l'adhésion, les commentateurs propagandistes détournent l'attention des utilisateurs, inondent les internautes chinois de messages favorables au parti-État qui éclipsent les autres messages (y compris les R-DATA, comme les messages opposés au PCC)¹²²⁹. La pluralisation de A-DATA a ici pour intérêt d'occulter les contenus refusés par le gouvernement, dans le cadre d'une bataille des chiffres par le nombre de messages promus.

La pluralisation de contenus propagandistes est aussi une technique mobilisée par la Fédération russe. On l'a déjà illustré avec le cas des trolls farms créées par l'État fédéral russe pour fabriquer de fausses informations destinées à tromper l'opinion publique américaine lors de l'élection présidentielle états-unienne de 2016. On a vu aussi que la Fédération a organisé l'apparition de « TikTok houses » depuis l'intervention militaire russe en Ukraine de 2022. Les TikTok houses ont pour mission de démultiplier le nombre de contenus patriotiques hébergés par TikTok, et elles sont le fruit d'une coopération d'initiatives privées et publiques comme c'est souvent le cas en Russie.

¹²²⁷ HAN Rongbin, *Challenging the Regime, Defending the Regime: Contesting Cyberspace in China*, Thèse en sciences politiques, Université de Californie, Berkeley, 2012, p. 71s. ; BANDURSKI David, « China's Guerrilla War for the Web », *Far Eastern Economic Review*, vol. 171, juil. 2008, p. 41s. ; RICHERI Guseppe, « L'Internet en Chine, entre État et opinion publique », *Les Enjeux de l'information et de la communication*, n° 19, 2018, p. 21-33

¹²²⁸ KING Gary, PAN Jennifer et ROBERTS Margaret E., « How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument », *American Political Science Review*, vol. 111, 2017, p. 494

¹²²⁹ ARSÈNE Séverine, « Complexité du nationalisme numérique en Chine », *Perspectives chinoises*, n° 2020-2, juin 2020 : « Les [commentateurs propagandistes] se lancent rarement dans des échanges approfondis avec d'autres utilisateurs et se contentent de répéter des éléments de langage rabâchés que plus personne ne prend vraiment au sérieux. Voilà qui semble contreproductif. Néanmoins, comme l'ont relevé d'autres chercheurs, le principal objectif pourrait simplement être de détourner ou repousser les lecteurs plutôt que de les convaincre (King, Pan et Roberts 2016). »

En février 2020, l'influenceur russe Ivan Morozov, alors âgé de 21 ans, fonde l'agence One Media. Avant de participer aux TikTok houses de 2022, One Media entretenait des partenariats avec le journal d'État Russia Today (RT) et avec l'organisation « Russie-Terre d'Opportunités »¹²³⁰. Pour RT, One Media s'est engagée à « *publier des tiktoks pour RT sous le hashtag #jemesouviens [япомню] afin de promouvoir l'idée du « Régiment Immortel » auprès des jeunes, selon le site web de l'agence [agencyone.ru]* »¹²³¹. Quant à Russie-Terre d'Opportunités, il s'agit d'une organisation autonome à but non lucratif créée par le Bureau présidentiel en 2018, présidée par le directeur de l'École supérieure d'administration de l'État à l'Académie russe de l'économie nationale (Alexei Komissarov), et spécialisée dans la fourniture de services dans le domaine de l'éducation¹²³². Par une liste d'instructions qu'il approuve le 26 juin 2022, le président Vladimir Poutine charge Russie-Terre d'Opportunités : d'accorder une bourse d'étude et des voyages aux adolescents et étudiants qui « *participent systématiquement à des activités sociales visant à former l'identité civique panrusse chez les enfants et les jeunes, le patriotisme et la responsabilité civique (...)* » ; et de définir « *dans les établissements d'enseignement supérieur, des locaux dédiés* » à l'accueil de ces adolescents et étudiants pour leur permettre de diffuser des contenus patriotiques sur internet¹²³³. On ignore exactement en quoi consiste le partenariat de One Media avec Russie-Terre d'Opportunités, mais certains blogueurs membres de l'agence One Media – comme le tiktoker Timich (@timiiich) – ont tourné leurs vidéos dans des salles de classe universitaires¹²³⁴.

Appelés « TikTok houses », ces locaux réservés aux jeunes pour la diffusion de contenus patriotiques ne semblent pas avoir convaincu massivement la jeunesse russe de la légitimité de la guerre. En effet, le premier public-cible de cette propagande est la jeunesse. Or, c'est précisément chez les Russes âgés de 18 à 24 ans que le soutien aux forces armées russes en Ukraine a le plus reculé entre février 2022 et mai 2023, passant de 71% à 62% – tandis que l'opposition aux forces armées a augmenté d'au moins 10 points dans cette tranche d'âge, passant de 19% à 29% (hors les 9% qui refusent de se prononcer)¹²³⁵. Il apparaît donc que la

¹²³⁰ POZYCHANYUK Valeria, « TikTok patriotique, Big Techs et censure et premiers signes de récession dans l'informatique » (Патриотичный TikTok, бигтехи и цензура и первые признаки рецессии в IT), *The Bell*, 24 juil. 2022

¹²³¹ PANKRATOVA Irina, « Guerre et paix dans TikTok. Comment les "maisons tiktok" russes se sont transformées en bureaux de propagande militaire » (« Война и мир в TikTok. Как российские «тикток-хаусы» превратились в офисы военной пропаганды »), *The Bell*, 22 juil. 2022

¹²³² *Ibid.* Au sens de la loi russe, une « organisation autonome sans but lucratif » (Автономная некоммерческая организация, АНО ou ANO en anglais) est une organisation « *créée par des citoyens et/ou des personnes morales [y compris des municipalités] sur la base de contributions volontaires de biens* » « *dans le but de fournir des services dans les domaines de l'éducation, des moyens de subsistance, de la santé, de la culture, de la science, du droit, du sport et dans d'autres domaines* » (Loi fédérale n° 7-FZ sur les associations sans but lucratif (Федеральный закон "О некоммерческих организациях") du 12 janvier 1996, art.7 et 10)

¹²³³ Liste d'instructions faisant suite à la réunion du Conseil de surveillance de l'ANO « Russie-Terre d'Opportunités » (Перечень поручений по итогам заседания наблюдательного совета АНО «Россия-страна возможностей») du 26 juin 2022, art. 1^{er}, sur *Kremlin.ru*

¹²³⁴ PANKRATOVA I., « Guerre et paix dans TikTok » (Война и мир в TikTok), préc. *The Bell*, 2022

¹²³⁵ Par comparaison, le soutien à la guerre toutes tranches d'âge confondues est passé de 81% à 76% sur la même période, de 73% à 69% chez les 25-39 ans, de 83% à 79% chez les 40-54 ans et de 86% à 83% chez les plus de 55 ans : Centre Levada, « Conflit avec l'Ukraine » (Конфликт с Украиной) [en

pluralisation des contenus de propagande par la coordination de TikTok houses a été peu voire très peu efficace pour susciter l'adhésion des 18-24 ans à l'intervention militaire russe en Ukraine. On a déjà expliqué le degré élevé de soutien en Russie par : la politique militaro-patriotique menée par la Fédération depuis 2009 dans les médias traditionnels (télévision, journaux, radio) et dans les écoles ; et le soutien passif d'une grande partie de la population un peu désabusée par ce conflit, qui préfère ne pas en entendre parler¹²³⁶. Entre ces deux paramètres importants, on doute que les TikTok houses aient été un facteur déterminant pour faire adhérer la population russe, principalement les jeunes adultes, aux actions des forces armées russes.

Tant en Russie qu'en Chine, on ignore toutefois si la pluralisation de contenus de propagande a été efficace pour occulter les messages contestataires. Que cette technique ait été ou non efficace pour éclipser les messages contestataires, elle semble du moins avoir été inefficace pour réduire l'opposition russe à la guerre en Ukraine comme on l'a vu (et l'opposition au gouvernement chinois comme on le verra). Conformément la règle selon laquelle la pluralisation de A-DATA doit son succès à la satisfaction de la demande par l'offre de A-DATA, on explique cet échec des TikTok houses par le fait que l'offre (messages de propagande) n'a pas satisfait la diversité d'intérêts des utilisateurs russes. On a en revanche constaté, avec l'essor technologique chinois, que la pluralisation de A-DATA peut s'avérer très efficace si l'offre de A-DATA satisfait la demande des prescripteurs en ligne (utilisateurs, programmeurs, opérateurs, gestionnaires de serveurs, administrateurs d'applications et fabricants).

C) Avantages et inconvénients de la pluralisation de A-DATA

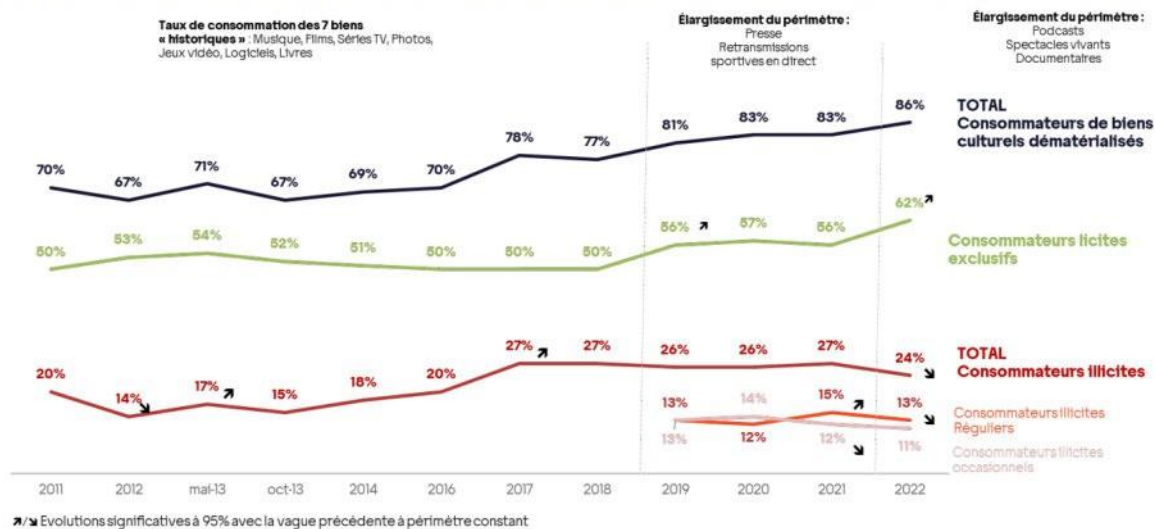
1. Premier avantage de la pluralisation de A-DATA : l'augmentation des capacités des utilisateurs à consommer légalement

On identifie deux principaux avantages et inconvénients à la pluralisation de A-DATA. Premier avantage : **la pluralisation de A-DATA augmente la quantité de A-DATA accessibles par l'utilisateur, donc augmente la capacité de l'utilisateur d'accéder à une A-DATA**. Un exemple type est celui de l'offre légale de vidéos à la demande (Netflix, Amazon Prime Video, Disney Plus, HBO Max...), ou de l'offre légale de musiques (Spotify, Sound Cloud, Deezer, YouTube, Tidal...), qui confèrent aux internautes la capacité de consommer légalement des biens culturels sans devoir utiliser un mode illicite de consommation (*i.e.* ne respectant pas les droits d'auteur). La pluralisation de l'offre légale de biens culturels a-t-elle eu pour effet de réduire la consommation illicite ? En France, les résultats sont *a priori* décevants :

ligne], *Levada.ru*, 31 mars 2022 ; Centre Levada, « Conflit avec l'Ukraine : évaluation de mai 2023 » (Конфликт с Украиной: оценки мая 2023 года), *Levada.ru*, 1^{er} juin 2023. Dans le détail, sur cette période, la proportion des Russes de 18-24 ans qui soutiennent « *certainement* » les actions de forces armées russes en Ukraine a progressé de 4 points (de 29% à 33%), mais la proportion des 18-24 ans qui soutiennent « *plutôt* » ces actions a chuté de 13 points (de 42% à 29%) ; le pourcentage des 18-24 ans qui ne soutiennent « *plutôt pas* » ces actions a augmenté de 7 points (de 9% à 16%), et le pourcentage de 18-24 ans qui ne la soutiennent « *certainement pas* » a crû de 3 points (de 10% à 13%).

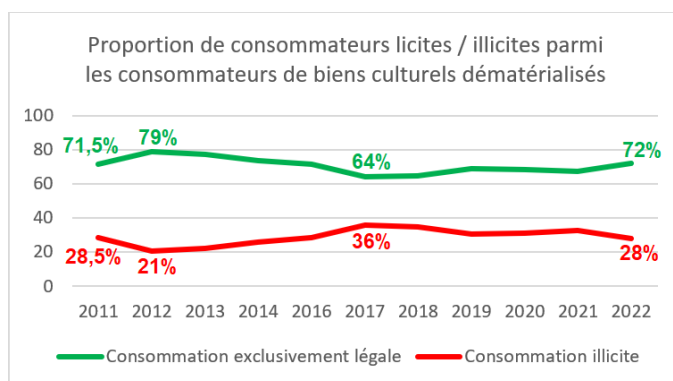
¹²³⁶ *Ibid.* Dès mars 2022, plus d'un tiers (35%) de la population russe ne suivaient pratiquement pas voire pas du tout les événements en Ukraine ; en mars 2023, ce désintérêt pour les événements en Ukraine atteint presque la moitié (45%) de la population russe, ce qui traduit l'absence d'implication active des citoyens dans le soutien patriotique

Part des internautes français qui consomment légalement / illégalement des biens culturels dématérialisés 2011-2022



Source : Arcom – Baromètre de la consommation 2022.

D'après les données de l'Arcom (ex-Hadopi), 24% des internautes français déclaraient avoir consommé illégalement au moins un bien culturel en 2022, soit 4% de plus qu'en 2011. Cela signifie que l'échelle de diffusion de la R-DATA « consommation illicite de biens culturels dématérialisés » a considérablement augmenté depuis 2011 : d'environ 10,15 millions (20% des 50,8 millions d'internautes français en 2011), le nombre de consommateurs illicites est passé à 14,6 millions en 2022 (24% des 60,9 millions d'internautes français en 2022). Non seulement la pluralisation de l'offre légale n'a pas empêché la hausse de l'échelle de diffusion de la R-DATA en cause, mais elle ne semble pas non plus avoir eu d'effet positif sur le rapport consommateurs licites / illicites¹²³⁷.



En effet, d'après les données de l'Arcom, en 2011, 71,5% des consommateurs de biens culturels dématérialisés consommaient exclusivement une offre légale, tandis que 28,5% consommaient une offre illicite (5,7% exclusivement de toute offre légale, 22,8% simultanément avec une offre légale)¹²³⁸. En 2022, 72% des consommateurs de biens culturels dématérialisés consommaient exclusivement une offre légale, tandis que 28% consommaient

¹²³⁷ Les chiffres rapportés dans le schéma ci-dessous ont été calculés à l'aide du schéma précédent. Par exemple, en 2012, il existait 14% d'internautes consommant illégalement des biens culturels pour un total de 67% d'internautes consommant des biens culturels ; par conséquent, les consommateurs illicites représentaient $14 \times 100 / 67 = 21\%$ de la totalité des internautes consommant des biens culturels. Les chiffres calculés correspondent à ceux donnés par le Baromètre des Usages (BU) régulièrement publié par la Hadopi depuis 2011.

¹²³⁸ Hadopi, « Hadopi, biens culturels et usages d'Internet : pratiques et perceptions des internautes français – BU 4 », sur *Hadopi.fr*, janv. 2014, p. 30

une offre illicite (2,3% exclusivement, 25,7% de façon mixte) ¹²³⁹ . En d'autres termes, proportionnellement au nombre de consommateurs de biens culturels dématérialisés, la part de consommateurs illicites n'a quasiment pas diminué (passant de 28,5% à 28%) sur une période de onze ans. Elle a même fortement augmenté de 15 points entre 2012 et 2017, passant de 21% à 36%. On explique cette hausse principalement par deux facteurs : l'essor de nouveaux modes d'accès très faciles d'utilisation pour consommer des biens culturels illégalement – le streaming et le téléchargement direct qui ont progressivement supplanté le téléchargement P2P¹²⁴⁰ ; et le succès tardif de l'offre légale de musiques, de films et de séries TV en France, qui débute vraiment entre 2016 et 2017¹²⁴¹ . En effet, depuis 2017, la part d'internautes français abonnés à un service de vidéo à la demande est passée de 9% à 51% en 2022 et, depuis 2016, la part d'internautes français abonnés à un service de musiques en streaming est passé de 7,5% à 23% en 2022 ¹²⁴² . Cette forte croissance s'est accompagnée d'une décline significative de la

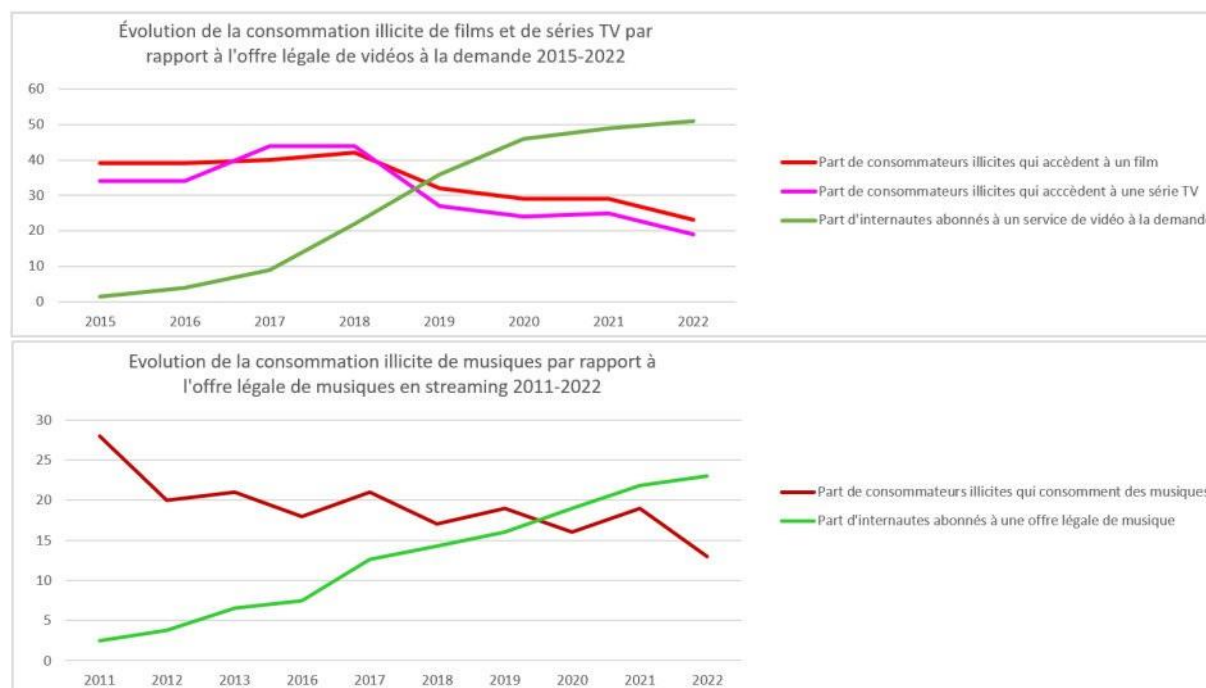
¹²³⁹ Arcom, « Baromètre de la consommation des biens culturels dématérialisés », 2022, p. 36

¹²⁴⁰ En 2012, 7,5 millions d'internautes français consommaient illégalement chaque mois un ou plusieurs biens culturels dématérialisés par téléchargement direct, 6,1 millions par téléchargement P2P et 4,2 millions par streaming – soit un total de 17,97 millions d'internautes (cette somme inclut évidemment des doublons car environ 7,4 millions d'internautes français consommant illégalement des biens culturels dématérialisés, ce qui signifie que chaque consommateur en illégalité utilisait en moyenne 2,42 modes d'accès illicites). En 2015 cette somme de 17,97 millions atteignait plus de 19 millions d'internautes (7,6 millions en téléchargement direct, 5,8 millions en téléchargement P2P, 5,4 millions en streaming), contre 15,4 millions en 2009 (8,3 millions en téléchargement P2P, 4,4 millions en téléchargement direct et 2,5 millions en streaming). Les modes d'accès illicites à des biens culturels ont donc gagné plus d'un million d'internautes français entre 2012 et 2015, alors que le nombre d'internautes français recourant à ces modes d'accès s'était stabilisé entre 2011 (17,97 millions) et 2012 (17,97 millions). Sur ces chiffres, v. Hadopi, « Rapport d'activité 2015-2016 », 10 janv. 2017, p. 44

¹²⁴¹ Netflix ne s'est lancée sur le marché français qu'à la fin de l'année 2014. En 2015, Netflix totalisait 900 000 abonnés en France, contre 613 000 pour Canalplay (CSA, « Netflix : Résultats annuels 2015 et perspectives 2016 », mars 2016, p. 14-15). La même année, les films et séries TV étaient de loin les biens culturels les plus consommés illégalement : 39% des consommateurs en illégalité consommaient des films, 34% des séries TV, et 18% de la musique (Hadopi, « Rapport d'activité 2015-2016 », préc., 2017, p. 37). Le faible nombre d'abonnés à l'offre légale de films et séries TV, couplé avec le fait que les films et séries TV étaient les biens culturels les plus consommés illégalement, illustrent une demande française non encore conquise par l'offre légale en 2015. En 2017, Canalplay annonçait 4,9 millions d'abonnés, Netflix dépassait le seuil des 3 millions, et OCS en comptait 2,9 millions (« Netflix tout près des 3,5 millions d'abonnés en France », *Libération*, 6 avril 2018). 2017 fut ainsi l'année durant laquelle l'offre légale de films et de séries TV a entamé son plein essor en France, ce qui correspond par ailleurs à l'année clôturant la hausse de la consommation illicite débutée en 2012.

¹²⁴² Pour l'évolution du nombre d'abonnés aux services de vidéos à la demande : Arcom, « Baromètre de la consommation des biens culturels dématérialisés », 2022, p. 29 ; Hadopi, « Baromètre de la consommation des biens culturels dématérialisés », 2021, p. 41 ; Hadopi, « L'Essentiel n°3 », 3 sept. 2017, p. 4. Pour l'évolution du nombre d'abonnés aux services de musique en streaming : Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022, p. 58

proportion de consommateurs illicites qui consommaient des films, des séries TV et des musiques.



On remarque que **la consommation illicite de musiques, de films et de séries TV diminue à mesure que les internautes français adoptent des services légaux de vidéos à la demande** (Netflix, Amazon Prime Video, Disney+, Canal+ VOD, HBO, OCS...) **et de musique en streaming** (Spotify, Apple Music, Amazon Music, YouTube Music, Tidal...). Alors que, en 2017, 44% de consommateurs illicites consommaient illégalement des séries TV et 40% des films, ils n'étaient respectivement plus que 19% (-25%) et 23% (-17%) en 2022¹²⁴³ ; sur la même période, la part d'internautes abonnés à une offre légale de vidéo à la demande est passée de 9% à 51% (+42%). Le constat est le même pour l'offre légale de musique : après que l'offre légale de musiques en streaming ait dépassé les 10% d'internautes abonnés en 2017 (12,5%), la part de consommateurs illicites qui consommaient de la musique illégalement est passée de 21% à 17% entre 2017 et 2018 ; cette dernière part a progressivement diminué jusqu'à 13% en 2022 (-8% depuis 2017), soit son niveau historique le plus bas¹²⁴⁴, quand 23% des internautes étaient abonnés à une offre légale (+10,5% depuis 2010). En-dehors des offres payantes par abonnement, l'offre légale gratuite de musiques a percé au début des années 2010 (le nombre d'utilisateurs français de YouTube est passé de 15 millions en 2010 à 23 millions en 2011 puis 27 millions en 2012, et celui de Deezer est

¹²⁴³ Pour les chiffres de la consommation illicite de films et de séries TV depuis 2015, v. : Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2017 – BU 7 », sept. 2017, p. 32 ; Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2018 – BU8 », avr. 2018, p. 40 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2019 », déc. 2019, p. 32 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2020 », févr. 2021, p. 35 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2021 », nov. 2021, p. 49 ; Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022, p. 36

¹²⁴⁴ Pour les chiffres de la consommation illicite de musiques, v. *ibid.*

passé de 7 millions à 26 millions entre 2010 et 2012¹²⁴⁵) – ce qui coïncide avec la baisse importante de la consommation illicite de musique enregistrée entre 2011 et 2012.

La baisse de la consommation illicite de musiques, de films et de séries TV coïncide donc avec l'adoption progressive de l'offre légale de ces mêmes biens culturels. Pour autant, l'offre légale a-t-elle joué un rôle causal dans la baisse de la consommation illicite ? Les données rapportées par la Hadopi-Arcom semblent y répondre par l'affirmative. Premièrement, les anciens et actuels consommateurs illicites de biens culturels qui ont réduit ou arrêté de fréquenter des services se sont principalement reportés sur des sites légaux : en juin 2017, 39% d'entre eux déclaraient consommer davantage sur des sites légaux (53% parmi les anciens illicites depuis moins de cinq ans), 25% déclaraient consommer moins de produits culturels (34% parmi les anciens illicites), 20% récupérer les biens culturels auprès d'autrui (hors partage d'abonnements, par exemple par clé USB, disque dur, stockage cloud...), 8% consommer davantage en streaming qu'en téléchargement, 5% fréquenter d'autres sites illégaux, 4% consommer plus en téléchargement qu'en streaming, et 2% déclaraient d'autres moyens pour consommer leurs biens culturels¹²⁴⁶. En d'autres termes, la baisse de fréquentation de sites illégaux n'est pas due principalement au fait que les consommateurs illicites aient cessé de consommer des biens culturels, ni même au fait qu'ils ont obtenu leurs biens culturels par autrui, et encore moins au fait qu'ils aient diminué leur consommation de streaming ou de téléchargement ou qu'ils aient changé de sites illégaux ; cette baisse de fréquentation des sites illégaux est due principalement au fait que les consommateurs illicites se sont dirigés vers l'offre légale. Cela signifie que la baisse observée de la consommation illicite s'est principalement reportée sur la hausse de l'offre légale : l'offre légale semble de loin la première option choisie par les consommateurs illicites qui réduisent et surtout par ceux qui arrêtent leur fréquentation de sites illicites.

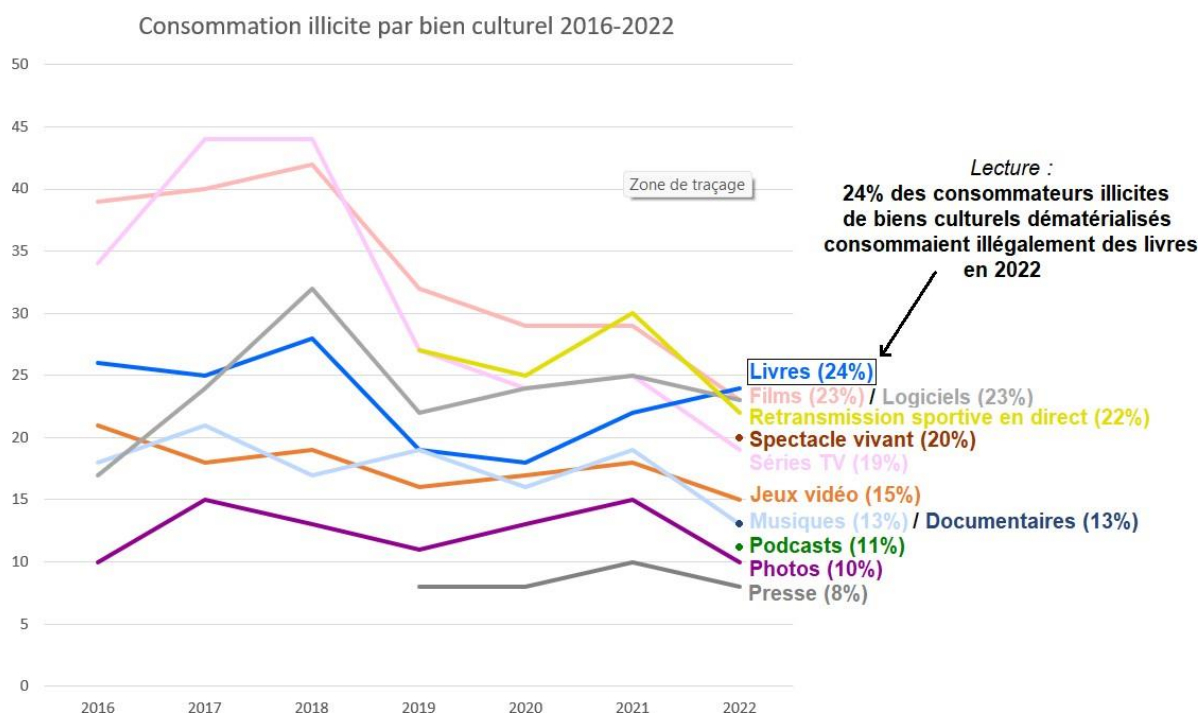
Deuxièmement, les secteurs dans lesquels l'offre légale s'est le plus développée durant les années 2010 (musique en streaming et vidéo à la demande) sont aussi ceux dans lesquels la consommation illicite a le plus diminué depuis 2017 : entre 2017 et 2022, la part de consommateurs illicites qui consommaient illégalement des séries a chuté de 25%, de 17% pour les films, de 8% pour la musique, de 5% pour les photos, de 3% pour les jeux vidéo, de 1% pour les logiciels et de 1% pour les livres (dont la consommation illicite est toutefois en train de reprendre fortement, notamment via les mangas)¹²⁴⁷. La consommation illicite de biens culturels a donc baissé là où l'offre légale a le plus conquis la demande. De plus, la musique, les séries TV et les films affichent depuis 2017 une tendance à la baisse assez régulière (continue pour les séries TV et les films,

¹²⁴⁵ « Les sites de vidéo les plus populaires en France » [en ligne], *Journal du Net*, 3 avr. 2010 ; Médiamétrie, « Le Top 15 des Brands Players les plus visités en France », sept. 2011 ; Médiamétrie, « Le Top 15 des Brands Players les plus visités en France », avr. 2012 ; ROZAT Pascal, « Deezer : la rentabilité au bout du chemin ? », *La revue des médias*, 2 mars 2011 ; SANYAS Nil, « Deezer compte multiplier par 13 son nombre d'abonnés Premium » [en ligne], *NextInPact*, 10 oct. 2012

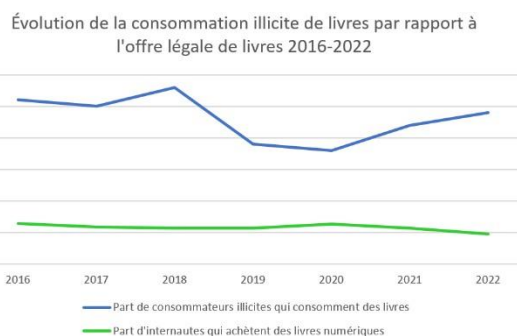
¹²⁴⁶ Hadopi, « Étude sur les risques encourus sur les sites illicites », juin 2017, p. 57

¹²⁴⁷ Pour l'évolution de la consommation illicite par bien culturel depuis 2016, v. Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2017 – BU 7 », sept. 2017, p. 32 ; Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2018 – BU8 », avr. 2018 p. 40 Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2019 », déc. 2019, p. 32 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2020 », févr. 2021, p. 35 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2021 », nov. 2021, p. 49 ; Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022, p. 36

par à-coups pour la musique), assez contrôlée. Inversement, les biens culturels pour lesquels l'offre légale a peu conquis le marché obéissent à des tendances beaucoup plus incontrôlées :



Seuls les jeux vidéo semblent connaître une baisse contrôlée similaire à la musique (passant de 21% en 2016 à 15% en 2022), probablement en raison du développement intense de l'offre légale sur ce segment depuis la fin des années 2010-début 2020 (achats dématérialisés de jeux directement depuis la console, achats dématérialisés de jeux sur ordinateur avec le succès des boutiques en ligne de jeux vidéo comme Steam ou Epic Games Store...) ¹²⁴⁸. Inversement, dans le secteur des livres (graphique ci-contre) où l'offre légale n'a pas émergé sur le marché français – *i.e.* n'a pas été adoptée par plus de 10% des internautes français – et a même régressé entre 2020 et 2022, la courbe d'évolution de la consommation illicite est beaucoup plus incontrôlée, beaucoup plus dépendante du renouvellement des centres d'intérêt de la demande ¹²⁴⁹. Ainsi, la hausse récente et soudaine de



¹²⁴⁸ TROUVÉ Pierre, « Jeu vidéo : forte hausse des ventes de jeux dématérialisés en France en 2020 », *Le Monde*, 3 mars 2021

¹²⁴⁹ Pour les données du graphique ci-contre, on s'est appuyé sur les chiffres du ministère français de la culture (pourcentage de la population française ayant acheté des livres numériques) qu'on a rapportés au nombre d'internautes français : Ministère de la culture, « Chiffres-clés du secteur du livre 2016-2017 », mars 2018, p. 2 ; Ministère de la culture, « Chiffres-clés du secteur du livre 2023 », 20 avr. 2023

la consommation de mangas contribue très probablement à la hausse de la consommation illicite de livres depuis 2020, faute d'une offre légale de mangas largement adoptée aujourd'hui¹²⁵⁰.

En somme, deux constats nous amènent à conclure que **l'offre légale a effectivement eu un rôle causal dans la baisse de la consommation illicite de biens culturels en ligne depuis 2017 en France** : (i) les consommateurs illicites qui ont cessé leur consommation illégale se sont principalement dirigés vers l'offre légale en 2017, date à laquelle les offres légales de vidéos à la demande et de musiques ont émergé en France (donc la majorité de la baisse de la consommation illicite s'est directement reportée sur la hausse de l'offre légale) ; (ii) les biens culturels dont la consommation illicite a le plus diminué (séries TV, films, musiques, jeux vidéo) sont ceux qui ont suscité le plus d'adhésion à l'offre légale (services de vidéos à la demande et de musiques en streaming) et, inversement, les biens culturels dont la consommation illicite a le moins diminué (livres, logiciels) sont ceux qui ont suscité le moins d'adhésion à l'offre légale. Par conséquent, **si la consommation illicite s'est maintenue à un niveau élevé entre 2017 et 2022** (un quart des internautes français), **ce n'est pas en raison de l'échec de l'offre légale de vidéos à la demande, de musiques en streaming et de jeux vidéo**. Sur cette période, là où l'offre légale a été la plus adoptée, elle fut le principal facteur de réduction de la part de consommateurs illicites qui consommaient illégalement des séries TV (-25%), des films (-17%), de musiques (-8%) et de jeux vidéo (-5%), ce qui a provoqué une baisse ininterrompue de la part de consommateurs illicites parmi l'ensemble des consommateurs de biens culturels (-8% depuis 2017). *A contrario*, là où l'offre légale fut la moins adoptée, la part de consommateurs illicites qui consommaient illégalement des livres (-2% depuis 2016), des photos (= depuis 2016) et des logiciels (+6% depuis 2016) a très peu diminué, et son évolution n'est pas contrôlée. **Il semble donc que le maintien d'un niveau élevé de consommation illicite soit principalement dû à l'insatisfaction de la demande par l'offre légale de ces biens culturels**. Il nous apparaît alors important de garantir l'émergence de l'offre légale des biens culturels là où la demande est insatisfaite (mangas, logiciels, retransmissions sportives en direct...) et de continuer à enrichir l'offre légale des autres biens culturels pour espérer une diminution à long terme de la consommation illicite.

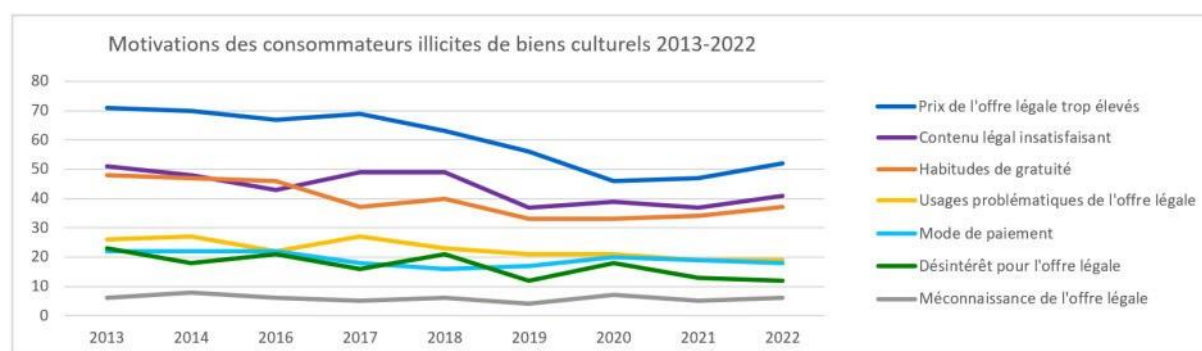
2. Deuxième avantage de la pluralisation de A-DATA : la réduction du risque de contournement

En plus d'avoir effectivement réduit la consommation illicite de films et de séries en augmentant la capacité de l'utilisateur à consommer légalement ces biens culturels, la pluralisation de l'offre légale présente un deuxième avantage vis-à-vis de la consommation illicite : **la pluralisation de A-DATA facilite la satisfaction de la demande par l'offre, donc limite le risque de contournement**. On a déjà observé cet avantage en Chine avec la pluralisation des applications chinoises : cette technique a largement réduit l'intérêt que pourraient trouver les internautes chinois à contourner les restrictions d'accès aux applications étrangères.

On observe le même phénomène avec l'offre légale de VàDA. Pour identifier les freins à la consommation licite de biens, la Hadopi-Arcom interroge depuis 2011 les consommateurs illicites sur leurs motivations, classées en 7 catégories : le prix de l'offre légale (motivation qui comprend les items « le prix des abonnements est trop élevé » et « le prix à l'unité est trop élevé ») ; le contenu

¹²⁵⁰ En 2022, sur 400 millions de chapitres de mangas lus chaque année en France, plus de 200 millions l'étaient illégalement (les mangas sont téléchargés par chapitre) : BAYON Arthur, « Enquête sur le "scantrad", le piratage de mangas à l'échelle industrielle », *Le Figaro*, 3 juin 2022

insatisfaisant de l'offre légale (« ce n'est pas facile de trouver l'œuvre que je cherche », « les sites légaux proposent une offre trop limitée », « impossible de découvrir des nouveautés rapidement », et « pas toujours possible de tester / visualiser le contenu avant l'achat ») ; les habitudes de gratuité des consommateurs (« pourquoi devrais-je payer ce que je peux obtenir gratuitement ? » et « par habitude, j'ai toujours consommé de façon gratuite sur internet ») ; l'usage problématique de l'offre légale (« les sites légaux ne sont pas faciles à trouver », « les sites légaux ne sont pas faciles à utiliser », « les verrous numériques (DRM) empêchent de faire des sauvegardes ») ; le mode de paiement (« j'ai peur de communiquer mes données bancaires » et « je ne possède pas de carte bancaire ou d'autres moyen de paiement en ligne ») ; le désintérêt des consommateurs pour l'offre légale (« pas besoin d'aller sur des sites légaux pour des contenus qui m'intéressent peu ») ; et enfin leur méconnaissance de l'offre légale (« je ne connais pas de sites légaux »). On retrace ci-bas l'évolution des motivations des consommateurs illicites¹²⁵¹ :



Entre 2013 et 2022, sont en recul toutes les motivations qu'ont les consommateurs illicites de consommer illégalement : en 2022, 52% des consommateurs illicites expliquent leurs pratiques en raison des prix trop élevés de l'offre légale (contre 71% en 2013, -19%), 41% en raison du contenu légal insatisfaisant (51% en 2013, -10%), 37% en raison des habitudes de gratuité sur internet (48% en 2013, -11%), 19% en raison des usages problématiques de l'offre légale (26% en 2013, -7%), 18% en raison des modes de paiement (22% en 2013, -4%), 12% en raison du désintérêt pour l'offre légale (23% en 2013, -9%). En cumulant toutes les motivations déclarées par les consommateurs illicites en 2013, on aboutit à un pourcentage de 247%. Cela signifie que, parmi les sept catégories de motivation identifiées par la Hadopi, **chaque consommateur illicite avait en moyenne 2,47 raisons de consommer illégalement en 2013**. En 2022, la somme des motivations déclarées par les consommateurs illicites atteignait 185%, ce qui signifie que **chaque consommateur illicite avait en moyenne 1,85 raisons de consommer illégalement**. On notera que, en 2017, chaque consommateur illicite avait en moyenne 2,21 raisons de consommer illégalement des biens culturels dématérialisés.

Cette baisse de la motivation à consommer illégalement traduit la réussite de l'offre légale de VàDA pour satisfaire la demande française de films et séries TV. En effet, l'offre légale semble avoir été un facteur déterminant dans le recul de la motivation des consommateurs

¹²⁵¹ Pour les chiffres sur les motivations des consommateurs illicites, v. : « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2013 – BU 4 », oct. 2013, p. 44 ; Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2017 – BU 7 », sept. 2017, p. 33 ; Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2018 – BU8 », avr. 2018 p. 51 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2019 », déc. 2019, p. 57 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2020 », févr. 2021, p. 46 ; Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2021 », nov. 2021, p. 30 ; Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022, p. 41

illicites : (i) la plupart des motivations (prix élevé, contenu insatisfaisant, usages problématiques et désintérêt) des consommateurs illicites ont commencé à baisser fortement depuis 2017-2018, ce qui coïncide avec l'essor de l'offre légale de vidéos à la demande et de musiques en France ; (ii) cette baisse de motivation coïncide par ailleurs avec la baisse de la consommation illicite enregistrée depuis 2017, dont on a vu qu'elle était largement causée par le déploiement de l'offre légale de vidéos à la demande et de musiques ; (iii) depuis 2017, les années durant lesquelles la motivation des consommateurs illicites était la plus basse (en moyenne 1,8 raisons de consommer illégalement par consommateur illicite en 2019, 1,84 raisons en 2020, et 1,75 raisons en 2021) correspondent aux années où la part d'internautes abonnés à une offre légale de vidéos à la demande a le plus augmenté (hausse de 13% en 2019, de 14% en 2020 et de 10% en 2021), tandis que les années durant lesquelles la motivation des consommateurs illicites étaient la plus haute (2,21 motivations/consommateur illicite en 2017, 2,18 en 2018, et 1,85 en 2022 en légère hausse par rapport à 2021) correspondent aux années où la part d'internautes abonnés à une offre légale a le moins augmenté (hausse de 2% en 2017, et de 5% en 2018 et en 2022). À mesure que l'offre légale satisfait leurs besoins, les consommateurs illicites perdent leurs motivations à consommer illégalement. On en déduit que **l'adoption de l'offre légale a eu un effet positif non seulement sur la réduction de la consommation illicite, mais aussi sur l'affaiblissement des motivations à consommer illégalement des biens culturels.**

La baisse de motivation des consommateurs illicites est un paramètre crucial pour viser une baisse de la consommation illicite. En effet, moins les consommateurs illicites ont de raisons de consommer illégalement, plus la consommation illicite est fragile, *i.e.* susceptible d'abandonner ses pratiques illégales. Inversement, plus les consommateurs illicites ont de raisons de consommer illégalement (par ex., si chaque consommateur illicite a au moins 7 raisons de consommer illégalement), moins ces consommateurs sont susceptibles d'abandonner leurs pratiques illégales. Le nombre de motivations/consommateur illicite est donc un indicateur de la flexibilité ou de l'inflexibilité de la consommation illicite : plus ce nombre tend vers 1, plus la consommation illicite est flexible, susceptible de diminuer (chaque consommateur illicite n'a qu'une seule raison de consommer illégalement) ; plus le nombre de motivations/consommateur illicite augmente, moins la consommation illicite est flexible, donc plus elle menace de stagner en contournant les restrictions (chiffrement des œuvres protégées dans le cadre de DRM, blocages, filtrages, et suppressions de sites ou de contenus diffusant illégalement des œuvres protégées...). Depuis 2017, en affaiblissant leurs motivations, **l'offre légale a donc effectivement réduit le risque que les consommateurs illicites contournent les restrictions pour accéder illégalement à des films, séries TV, musiques et jeux vidéo.**

3. Inconvénients de la pluralisation de A-DATA

En augmentant les capacités des internautes (1^{er} avantage de la pluralisation de A-DATA) à consommer légalement des biens culturels, l'offre légale a permis de diminuer la consommation illicite de biens culturels en France sur les segments de marché où elle s'est déployée (films, séries TV, musiques, jeux vidéo) ; en satisfaisant la diversité d'intérêts de la demande (2^e avantage de la pluralisation de A-DATA), l'offre légale a permis de réduire le risque de contournement en diminuant la motivation des consommateurs illicites à consommer illégalement. Parallèlement à ces deux avantages, on reconnaît deux principaux inconvénients à la pluralisation de A-DATA. Premier inconvénient : **la pluralisation de A-DATA aggrave le risque de délaissement.** En effet, les A-DATA que le régulateur s'efforce de pluraliser peuvent être tout simplement ignorées par les prescripteurs numériques.

On a vu que tel fut le cas des commentateurs propagandistes chinois (« armée des 5 centimes ») et des TikTok houses russes, mais aussi de l'offre légale de livres et de logiciels en France. Or, dans la mesure où le succès de la pluralisation dépend essentiellement de l'adoption des A-DATA, la pluralisation peut se montrer vaine si les A-DATA ne sont pas adoptées. En ce sens, la plupart des services européens que l'UE a tenté de faire émerger (De-Mail, Qwant, Initiative européenne de paiement...) ont été délaissés par les internautes, et ces services n'ont donc pas pu contribuer à réduire la dépendance des utilisateurs européens aux services américains. De même, en Russie, on a vu que le service de partage de vidéos Rutube (MAU de 5-6 millions début 2023) et le réseau social russe de courtes vidéos Yappy (MAU de 3-6 millions début 2023) ont été délaissés par les internautes malgré les espoirs du gouvernement fédéral¹²⁵², et ne sont donc pas non plus parvenus à diminuer la dépendance des utilisateurs russes à YouTube (MAU de 70-73 millions en Russie début 2023) et à TikTok (MAU de 40-45 millions en Russie début 2023). Si le régulateur souhaite pluraliser les A-DATA, il se heurte donc à un risque élevé de délaissement qui peut rendre inefficace la pluralisation mise en œuvre.

Les A-DATA peuvent mettre beaucoup de temps à être adoptés, comme en témoignent le développement de l'offre légale de vidéos à la demande en France, l'essor des entreprises chinoises au cours des années 2000 et, de manière générale, la courbe d'évolution du MAU des applications. Aussi, le risque de délaissement peut être réduit si la pluralisation de A-DATA s'accompagne d'une stratégie très organisée à long terme pour que l'offre légale satisfasse la demande. Par exemple, il ne nous semble pas pertinent de miser sur un seul service (De-Mail, Qwant, Rutube, Yappy...) par segment de marché (boîtes de messagerie, moteurs de recherche, service de partage de vidéos, réseau social de partage de courtes vidéos...), car tout service est par essence susceptible de ne pas satisfaire la demande sur ce segment. En revanche, il nous semble plus approprié de stimuler (par la concurrence et/ou le protectionnisme) l'essor général de l'offre légale sur un ou plusieurs segments de marché, d'inciter fortement l'offre légale à consacrer d'importantes dépenses dans la R&D et dans la recherche fondamentale, et d'apporter un soutien financier conséquent (par des investissements et/ou des subventions) aux acteurs qui se démarquent grâce à leurs innovations et à la valeur ajoutée qu'ils créent. Les investissements publics nous semblent être un outil primordial pour appuyer une telle stratégie.

Le problème de cette stratégie réside dans le fait que les conditions concurrentielles sont aujourd'hui très inégales entre les applications en ligne comme on l'a rapporté. De nombreux États se heurtent à la difficulté de stimuler l'essor de leurs entreprises nationales face aux privilèges concurrentiels dont bénéficient les géants d'internet (moyens financiers, bases d'utilisateurs, stratégies d'insertion...). En Russie, Rutube peut difficilement rivaliser avec YouTube qui, fort de sa communauté d'utilisateurs russophones, attire davantage les créateurs de contenus à la recherche d'audience, les entreprises à la recherche de visibilité et les visiteurs grâce à la quantité phénoménale de créateurs de contenus et de vidéos qu'il propose à ses utilisateurs. Pour des raisons similaires, en Europe, Qwant pouvait difficilement rivaliser avec Google Search, De-Mail le pouvait difficilement avec Yahoo Mail, Hotmail/Live/Outlook puis Gmail etc. On insiste donc sur l'urgence de réformer les règles internationales de concurrence

¹²⁵² « Les autorités [fédérales russes] offrent aux YouTubers et aux TikTokers en herbe jusqu'à 1 700 dollars par mois pour transférer leur contenu vers Yappy et RuTube. (...) VK, RuTube et Yappy sont tous contrôlés par la société publique Gazprom Media, ce qui permet au gouvernement d'influencer plus facilement les plateformes » : TYAN Alexandra, « Russia is determined to make RuTube happen », *Code Media*, 22 fév. 2022

pour décentraliser la gestion des applications en ligne (régulation des stratégies d'insertion, stricte limitation des rachats et fusions, stricte limitation du nombre de segments de marché sur lesquels un même propriétaire d'applications peut se développer, obligation pour les systèmes d'exploitation de proposer plusieurs systèmes d'exploitation, navigateurs web, moteurs de recherche, magasins d'applications, services de stockage en cloud...). Si la concurrence est sclérosée, elle ne peut plus être un moyen de garantir l'essor d'entreprises nationales, et le moyen le plus efficace pour atteindre cet objectif devient alors le protectionnisme (à l'image des blocages et filtrages des services étrangers en Chine).

Que l'émergence de services en ligne nationaux résulte de la concurrence ou du protectionnisme, il s'agit dans tous les cas d'un long processus. C'est pourquoi il est quasiment impossible, pour un pays dont la population utilise largement des services en ligne étrangers, d'isoler du jour au lendemain son réseau national vis-à-vis des services étrangers : des entreprises nationales doivent être préalablement en mesure de satisfaire quasiment à elles seules la demande intérieure, sans quoi le risque de contournement est élevé¹²⁵³.

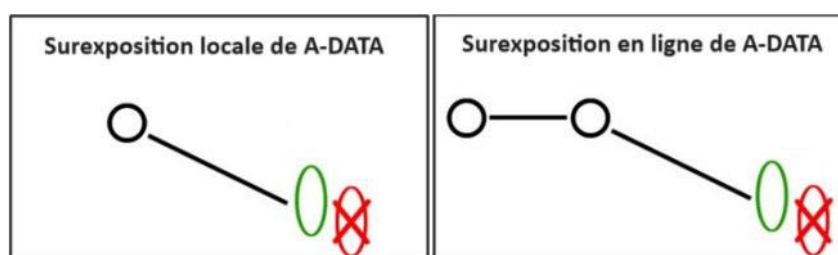
Outre l'aggravation du risque de délaissement, la pluralisation de A-DATA s'accompagne d'un deuxième inconvénient important : **l'accès à une A-DATA n'empêche pas l'utilisation de cette dernière pour produire ou consulter une R-DATA**. Par exemple, en Chine, l'offre légale de services en ligne (WeChat, TaoBao, QQ, Kuaishou, Douyin...) promue par l'État peut être utilisée pour diffuser massivement du cyberharcèlement, des contenus haineux, des contenus à caractère terroriste, des cyberattaques, des arnaques et autres fraudes commerciales... Ainsi, TaoBao héberge de nombreuses fraudes commerciales, et sert à de nombreux chercheurs pour

¹²⁵³ On l'a vu en Russie, où les blocages d'Instagram et de la fonction de téléchargement de vidéos sur TikTok ont été largement contournés et où le blocage de WhatsApp et de YouTube était difficilement envisageable dès lors qu'il s'agit de la messagerie instantanée et du service de partage de vidéos les plus utilisés en Russie. On le voit plus encore en Birmanie, où le régime militaire a opté pour des techniques de régulation extrêmement simplistes et grossières au lendemain du coup d'État de février 2021. La junte militaire a d'abord alterné les blocages de nombreux services étrangers (Facebook, Instagram, Twitter, YouTube...) avec les coupures d'internet, avant de généraliser la coupure du réseau internet national. L'armée s'est toutefois heurtée au premier inconvénient de la coupure, à savoir l'effondrement de l'économie nationale : l'accès distanciel aux banques, et plus généralement l'accès à internet par les entreprises birmanes, ont été rendus impossibles au point de coûter à l'économie birmane plus de 24 millions de dollars/jour (« Le coût désastreux du verrouillage d'internet en Birmanie » [en ligne], *ShareAmerica*, 24 mai 2021). Constatant la catastrophe économique de cette mesure, la junte militaire lève la coupure les 24-25 avril 2021, mais ordonne aux FAI de n'autoriser l'accès qu'à certains services admis (banques, entreprises birmanes, Telegram...) et d'empêcher l'accès à tous les autres services : « En Birmanie, Internet est de retour, la censure aussi », *Courrier international*, 29 avr. 2021. Or, ces restrictions sont massivement contournées par une grande partie de la population birmane : l'audience birmane de Facebook est passée de 28-30 millions (janvier 2021) à 20-22 millions (février 2022), puis à 15-17 millions (janvier 2023), celle de Messenger est passée de 18-20 millions (janvier 2021) à 15-17 millions (février 2022) puis à 12-14 millions (janvier 2023), et le nombre d'utilisateurs d'Instagram a même légèrement augmenté pour passer le 1,4 millions (janvier 2021) à 1,8 millions (février 2022) (WeAreSocial et Hootsuite, « Digital 2021. Myanmar », *DataReportal*, fév. 2021 ; WeAreSocial et Hootsuite, « Digital 2022. Myanmar », *DataReportal*, fév. 2022 ; WeAreSocial et Hootsuite, « Digital 2023. Myanmar », *DataReportal*, fév. 2023). De même, en janvier 2023, Twitter représentait 7,68% du trafic birman à destination des réseaux sociaux hors Telegram contre 2,69% en janvier 2021, et YouTube en représentait 4,4% en janvier 2023 contre 0,96% en janvier 2021 (« Social Media Stats Myanmar » [en ligne], *StatCounter*). Faute d'une offre légale nationale satisfaisante sur laquelle se reporter, plus de la moitié des internautes birmans a continué à consommer des services étrangers illicites. Après plus de deux ans et demi de restriction, la junte militaire n'est pas parvenue à isoler la Birmanie de ces services illicites.

expérimenter leurs algorithmes d'identification des fraudes¹²⁵⁴. Ou encore, WeChat et QQ comptent parmi les principaux canaux de diffusion du cyberharcèlement en Chine ; en 2021, au moins 18% des adolescents chinois de 12 à 18 ans avaient cyberharcélé quelqu'un, et 54,6% avaient été cyberharcelés par quelqu'un¹²⁵⁵. De même, les services légaux de musiques en streaming peuvent être utilisés à des fins frauduleuses. Depuis mai 2023, Spotify s'attaque ainsi à une pratique qui consiste, pour certains utilisateurs, à générer des milliers de musiques à l'aide d'applications d'intelligence artificielle (comme Boomy), à les déposer sur Spotify, à se servir de milliers de faux comptes d'auditeurs automatisés (robots en ligne) pour écouter ces musiques, puis à récupérer l'argent que leur verse Spotify proportionnellement à la diffusion des musiques¹²⁵⁶. La pluralisation de A-DATA peut donc être exploitée pour amplifier la diffusion de R-DATA.

D) La surexposition et la réutilisabilité d'une A-DATA

1. La surexposition d'une A-DATA



On décrira enfin succinctement les deux dernières techniques de régulation par augmentation qu'on a identifiées. On appelle « surexposition d'une A-DATA » la technique qui consiste à renforcer la visibilité d'une A-DATA. TikTok en a par exemple fait usage en Russie, en exploitant ses algorithmes pour surexposer les données propagandistes lorsque l'utilisateur recherche certains mots-clés comme « Ukraine » [v. *supra*].

On reconnaît deux principaux avantages et inconvénients à cette technique. Premier avantage : en augmentant la visibilité d'une A-DATA, **la surexposition valorise cette A-DATA auprès de l'utilisateur, donc augmente la probabilité que l'utilisateur y accède.**

¹²⁵⁴ ZHANG Ge, LI Zhao, HUANG Jiaming, WU Jia, ZHOU Chuan et YANG Jian, « eFraudCom: An E-commerce Fraud Detection System via Competitive Graph Neural Networks », *ACM Transactions on Information Systems*, vol. 40, juil. 2021. En 2016, TaoBao était « suspectée d'encourager les vendeurs à "brosser" de fausses ventes et a fait l'objet d'une enquête sur les fraudes possibles liées aux ventes "brossées". Une enquête a révélé que les vendeurs de Taobao qui pratiquent le "débroussaillage" payent de faux clients pour qu'ils passent commande et leur expédient ensuite des boîtes vides afin d'améliorer leur classement organique [i.e. leurs classement par les moteurs de recherche] », v. LONG Fei et LIU Yunchuan, « Fake Sales and Ranking Algorithms in Online Retail Marketplace with Sponsored Advertising », *Social Science Research Network*, 2022

¹²⁵⁵ ZHOU Shuhuan, « Status and Risk Factors of Chinese Teenagers' Exposure to Cyberbullying », *Sage Open*, vol. 11, oct. 2021

¹²⁵⁶ NICOLAOU Anna, « Spotify ejects thousands of AI-made songs in purge of fake streams », *Financial Times*, 9 mai 2023. Spotify ne paie pas les artistes à l'écoute (par ex. une écoute/un stream = 0,0033\$, comme l'évaluait Business Insider en 2020), mais à la diffusion des musiques : « nous calculons la part de diffusion en additionnant le nombre de fois où la musique détenue ou contrôlée par un détenteur de droits particulier a été diffusée et en divisant ce chiffre par le nombre totale de diffusions sur ce marché », v. MULROY Clare, « Spotify pay artists (sort of) but not per stream. Her's how it breaks down », *USA Today*, 22 oct. 2022

C'est là un gros avantage par rapport à la pluralisation. Tandis que la pluralisation augmente la possibilité d'accéder à une A-DATA, la surexposition en augmente la probabilité. Les deux techniques peuvent par ailleurs être combinées – par exemple, en surexposant des contenus propagandistes pluralisés par le régulateur.

Le plus souvent, la surexposition est mise en œuvre au moyen d'algorithmes de valorisation des contenus. Il est courant pour les applications en ligne de concevoir de tels algorithmes. Cette méthode est par exemple employée pour renforcer la visibilité des contenus publicitaires (« contenus sponsorisés »). Elle est aussi recourue par les moteurs de recherche, pour définir les règles de classement des résultats – ceux qui doivent figurer au début du classement et ceux qui doivent figurer à la fin. L'étude de ces règles de classement fait même l'objet d'un métier – Search Engine Optimization (SEO) –, dans le but d'exploiter ces règles pour valoriser un contenu ou un site web et le hisser parmi les premiers résultats affichés. La surexposition est encore pratiquée par Instagram pour valoriser sur le fil d'actualités de l'utilisateur les contenus originaux (qui émanent directement d'un créateur de contenus) au détriment des contenus existants (qui sont relayés par les utilisateurs), et ainsi renforcer la visibilité des créateurs de contenus quitte à réduire les interactions des utilisateurs¹²⁵⁷. En leur offrant une forte visibilité, Instagram attire de nombreux créateurs de contenus qui divertissent les utilisateurs du réseau social. On a vu que, en Russie, de nombreux créateurs de contenus et entreprises sont restés sur Instagram malgré son blocage en raison de la très forte valorisation dont ils bénéficient, qu'ils peinent à retrouver sur d'autres réseaux sociaux. Cela fait de la qualité des algorithmes de valorisation un atout concurrentiel décisif.

Dans un cadre politique, la surexposition est aujourd'hui principalement employée à des fins de propagande. Par exemple, sur Twitter, les communautés pro-Ukraine devançaient les communautés antisystème, complotistes et pro-Kremlin par le nombre de tweets et de retweets ; mais, depuis février 2023, le volume de tweets et de retweets des communautés antisystème et pro-Kremlin a dépassé celui recensé dans les communautés pro-Ukraine. En mars 2023, sur 2,1 millions de tweets contenant le mot « Ukraine », le doctorant Dusan Bozalka en identifie au moins 34% qui proviennent des communautés antisystème et pro-Kremlin, contre 28% qui proviennent des communautés pro-Ukraine. *« Ce renversement du rapport de force sur Twitter est susceptible d'accroître la visibilité conférée aux récits complotistes et pro-russes concernant l'Ukraine. Les algorithmes de recommandation de Twitter augmentent en effet la portée de certains messages selon leur popularité et la mobilisation qu'ils génèrent. (...) Les communautés pro-Kremlin et antisystème se coordonnent également pour amplifier artificiellement, grâce à des bots (comptes automatisés), la visibilité de certains messages ou comptes, tels que ceux évoquant les laboratoires ukrainiens. »*¹²⁵⁸.

Deuxième avantage de la surexposition : **en imposant à l'utilisateur la visibilité d'une A-DATA, la surexposition réduit le risque de délaissement**. C'est là encore une différence de taille avec la pluralisation de A-DATA, qui au contraire aggrave le risque de délaissement. Cette différence s'explique par le fait que la A-DATA surexposée s'affiche en principe auprès de l'utilisateur du service, tandis que la A-DATA pluralisée laisse à l'utilisateur le choix d'y

¹²⁵⁷ RAFFIN Estelle, « Instagram modifie son algorithme pour favoriser le contenu original : ce qui va changer » [en ligne], *Le Blogs du Modérateur*, 21 avr. 2022

¹²⁵⁸ BOZALKA Dusan, « Guerre en Ukraine : comment la Russie s'appuie sur la sphère complotiste pour diffuser sa propagande », *La Revue des médias*, 24 avr. 2023

recourir ou non. Une combinaison pluralisation + surexposition d'une même A-DATA permet donc de satisfaire la diversité de la demande, et d'augmenter la possibilité et la probabilité d'accès à cette A-DATA, tout en réduisant le risque de délaissement de ladite A-DATA.

On relève toutefois la décision pertinente de l'Union européenne d'obliger les très grandes plateformes et les très grands moteurs de recherche à fournir aux utilisateurs européens une ou plusieurs options aisément accessibles pour modifier ou influencer les principaux paramètres des systèmes de recommandation, ainsi qu'une ou plusieurs options pour désactiver les recommandations par profilage ¹²⁵⁹. Pour se conformer au Digital Services Act (DSA), l'entreprise Meta est allée jusqu'à proposer aux utilisateurs européens des options de désactivation complète de ses algorithmes de recommandation ¹²⁶⁰. En donnant à l'utilisateur plus de contrôle sur les recommandations, le DSA offre aux utilisateurs la possibilité de délaisser les contenus surexposés. Précisons néanmoins que la surexposition n'est pas nécessairement le fruit des algorithmes de recommandation et de profilage, et qu'il existe des règles de classement des informations (sur un moteur de recherche, un fil d'actualités...) auxquelles les utilisateurs peuvent plus difficilement échapper. Cela signifie que cette mesure du DSA est loin de neutraliser la difficulté des utilisateurs à délaisser une donnée surexposée, mais du moins elle relativise cette difficulté au délaissement.

En adoptant ces dispositions, l'UE se prive du même coup des principaux avantages de la surexposition de A-DATA par recommandation : si l'UE souhaite surexposer certaines A-DATA dans les recommandations des utilisateurs, ces derniers seront en mesure d'empêcher l'affichage de ces A-DATA. Le DSA réduit ainsi la probabilité que l'utilisateur accède à une A-DATA surexposée par recommandation, et augmente le risque de délaissement de cette A-DATA surexposée. Ces dispositions nous semblent pourtant pertinentes car, par la même occasion, elles réduisent la probabilité que l'utilisateur accède accidentellement à une R-DATA du fait de sa surexposition par recommandation et par profilage (contenus haineux, fausses informations ou cyberharcèlement surexposés...).

Inversement, on reconnaît deux principaux inconvénients à la surexposition. Premier inconvénient : contrairement à la pluralisation de A-DATA, **la surexposition de A-DATA** ne facilite pas la satisfaction de la diversité de la demande, et **s'accompagne donc d'un risque élevé de contournement si les A-DATA surexposées ne satisfont pas la demande**. Par exemple, si une application en ligne surexpose des publicités qui ne satisfont pas les utilisateurs, ces derniers peuvent contourner la surexposition de plusieurs moyens – en recourant à un bloqueur de publicités ¹²⁶¹, en se déconnectant d'internet pour les applications mobiles (*i.e.* sur smartphone) pour interrompre les flux publicitaires transmis par le serveur, en migrant vers une autre application... De même, si une application en ligne surexpose des contenus

¹²⁵⁹ Digital Services Act, art. 27 et 40

¹²⁶⁰ MARIN Jérôme, « Les internautes européens vont pouvoir désactiver complètement les algorithmes de recommandation de contenu de Facebook et Instagram », *L'Usine Digitale*, 22 août 2023

¹²⁶¹ En janvier 2022, 37% des internautes dans le monde utilisaient un bloqueur de publicités contre seulement 8-10% en 2016 : Hootsuite et WeAreSocial, « Digital 2023: Global Overview Report », *DataReportal*, janv. 2023 ; SCOTT Mark, « Use of Ad-Blocking Software Rises by 30% Worldwide » [en ligne], *The New York Times*, 31 janv. 2017 ; « Adblocking use continues to grow, led by Asia » [en ligne], *Campaign*, 3 mai 2021

propagandistes envahissants, une majorité d'utilisateurs peut vouloir éviter la propagande et migrer vers une autre application¹²⁶².

Deuxième inconvénient : **la surexposition de A-DATA peut provoquer la surexposition de R-DATA**. En effet, si une R-DATA s'inscrit dans les règles de surexposition, elle bénéficiera d'un fort gain de visibilité. Une illustration typique de cet inconvénient est incarnée par la R-DATA « production et accès à des contenus haineux ». En effet, la haine semble être l'un des sentiments qui se diffuse le plus rapidement sur internet dans les espaces publics de discussion, même en-dehors de toute intervention algorithmique. Les algorithmes qui valorisent les contenus selon le critère de leur diffusion réelle ou potentielle risquent donc de surexposer des contenus haineux, dès lors que ces derniers ont naturellement une forte propension à être diffusés.

La vitesse de diffusion des messages publics haineux est démontrée par une étude chinoise de 2013¹²⁶³. Dans cette étude, les chercheurs examinent 70 millions de messages publiés sur Weibo durant six mois en 2010. Ils analysent les émoticônes utilisées dans ces messages à travers quatre types d'émotions : la joie ; la colère ; le dégoût ; et la tristesse. En limitant leur cadre d'étude aux utilisateurs qui avaient au moins 30 interactions durant la période d'observation, ils évaluent la probabilité pour qu'un destinataire retourne un message colérique après avoir reçu un message colérique, la probabilité qu'un destinataire retourne un message joyeux après avoir reçu un message joyeux etc. Les chercheurs constatent une très faible corrélation concernant la tristesse et le dégoût. En revanche, ils ont découvert une forte corrélation du côté des messages joyeux, et une corrélation encore largement plus élevée du côté des messages colériques. En d'autres termes, il est bien plus probable qu'un message colérique suscite un message colérique, plutôt qu'un message joyeux suscite un message joyeux, qu'un message triste suscite un message triste, ou qu'un message dégoûté suscite un message dégoûté. Cette étude de 2013 est certes limitée à Weibo, mais elle évalue la diffusion de la haine d'après un paramètre indépendant de l'algorithme de Weibo – la réaction émotionnelle la plus probablement exprimée en réponse à un message public chargé émotionnellement. Surtout, elle confirme le processus par lequel la haine suscite la haine, déjà maints fois démontré dans de nombreux domaines scientifiques¹²⁶⁴.

Cette conclusion est confirmée en 2020 par une étude sur Gab, un réseau social qui a pour philosophie de ne pas censurer les messages publiés, très réputé pour attirer la droite antisystème américaine, les théories complotistes et les propos haineux (suprémacistes, racistes, homophobes, misogynes...). En se focalisant sur Gab, l'enquête permet d'isoler l'observation des comportements dans un environnement haineux et constate que : la quantité de contenus

¹²⁶² La migration est une configuration de contournement qu'on examinera plus loin

¹²⁶³ FAN Rui, ZHAO Jichang, CHEN Yan et XU Ke, « Anger is More Influential Than Joy: Sentiment Correlation in Weibo », *ArXiv*, 10 sept. 2013

¹²⁶⁴ En sciences juridiques, v. MINOW Martha, *Breaking the Cycles of Hatred*, Princeton University Press, 2003 ; en sciences psychologiques, v. LITTMAN Rebecca et LEVY PALUCK Elizabeth, « The Cycle of Violence: Understanding Individual Participation in Collective Violence », *Political Psychology*, vol. 36, fév. 2015, p. 76-99 ; en sciences linguistiques, v. RINN Michael, « Les discours de la haine en question : Autour de quelques ouvrages récents », *Argumentation et Analyse du Discours*, n° 29, 2022 ; en sociologie, v. KING Ryan D. et SUTTON Gretchen M., « High times for hate crimes: explaining the temporal clustering of hate-motivated offending », *Criminology*, vol. 51, août 2013, p. 871-894

haineux augmente exponentiellement par rapport à l'augmentation du nombre d'utilisateurs ; et les nouveaux utilisateurs, baignant dans un langage de haine croissante, deviennent eux-mêmes haineux à un rythme de plus en plus rapide¹²⁶⁵. Cette étude corrobore une conclusion en sciences psychologiques, d'après laquelle l'auteur de violences vit péniblement le fait d'en infliger, mais est encouragé à poursuivre voire à accroître la violence qu'il inflige s'il s'identifie à un groupe d'appartenance violent¹²⁶⁶. La production de contenus haineux alimente la production de contenus haineux par leurs auteurs (plus un auteur de contenus haineux en produit, plus il est susceptible d'en produire à l'avenir s'il s'identifie à un groupe haineux, comme le démontre l'étude sur Gab confirmée en psychologie) et par leurs destinataires (plus une personne se sent ciblée par des contenus haineux, plus il est probable qu'elle produise des contenus haineux, comme le démontre l'étude sur Weibo¹²⁶⁷).

Les contenus haineux ont donc pour atout naturel leur rapidité de diffusion, ce qui facilite leur valorisation par des algorithmes qui surexposent les contenus à forte diffusion potentielle ou réelle. On examine trois cas dans lesquels des algorithmes surexposent accidentellement des contenus haineux en récompensant les contenus à forte propension d'audience et/ou d'engagement. C'était le cas de l'algorithme de YouTube en 2018. Entre les 9 et 20 juin 2018, une équipe de chercheurs insère plusieurs requêtes controversées ([islam], [refugee], [trump] », « [(Bernie) sanders]», [Gamergate]...) dans la barre de recherche de YouTube, analysent le classement des vidéos proposées pour chacune des recherches, et tentent d'identifier des corrélations entre l'ordre des résultats et : (i) le nombre de vues cumulées par une vidéo ; (ii) la récence de la vidéo ; (iii) le nombre de commentaires qu'elle suscite ; (iv) le nombre de fois qu'est recherché le mot-clé (islam, refugee...) ; (v) le nombre de vidéos publiées auxquelles renvoie la recherche ; (vi) le nombre de changement de rangs des vidéos sur la période observée¹²⁶⁸.

Pour la requête [trump], le classement semble corrélé à la récence des vidéos, ou la récence des événements dont elles traitent (les vidéos les plus récentes sont privilégiées). Pour la requête [sanders], le classement semble corrélé à la nativité des vidéos (les vidéos provenant originellement de YouTube sont privilégiées), à la fréquence de publication de vidéos sur Bernie Sanders par les chaînes YouTube populaires, et à la récence des vidéos. Pour la requête [islam], le classement semble corrélé au nombre de vidéos publiées pour la requête et au nombre de fois qu'est recherchée la requête (le classement change à mesure que sont publiées de nouvelles vidéos et qu'est recherché le mot [islam]), de façon à s'aligner sur « *l'actualité qui suscite à la fois l'intérêt des téléspectateurs et la production de vidéos* » (tuerie d'Orlando à l'époque). Pour la requête [494yrie], soumise en période d'intensification de la guerre civile syrienne, le classement semble corrélé

¹²⁶⁵ MATHEW Binny, ILLENDULA Anurag, SAHA Punyajoy, SARKAR Soumya, GOYAL Pawan, MUKHERJEE Animesh, « Hate begets Hate: A Temporal Study of Hate Speech », *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, p. 1-24

¹²⁶⁶ LITTMAN Rebecca et LEVY PALUCK Elizabeth, « The Cycle of Violence: Understanding Individual Participation in Collective Violence », préc., *Political Psychology*, 2015

¹²⁶⁷ En-dehors d'internet, cette dernière conclusion selon laquelle les destinataires de violences sont plus susceptibles d'en produire a par ailleurs été confirmée en sciences des relations internationales. Dans le cadre de sa thèse, Katerina Tkavoca constate ainsi que le terrorisme domestique à motivation ethnique aggrave la guerre civile entre groupes ethniques et que, en retour, la guerre civile augmente la fréquence du nombre d'attaques terroristes : TKACOVA Katerina, *Hate Begets Hate; Violence Begets Violence: The Case of Domestic Terrorism on Behalf of Ethnic Groups*, Thèse, Université d'Essex, 2017.

¹²⁶⁸ RIEDER Bernhard, MATAMOROS-FERNÁNDEZ Ariadna et COROMINA Òscar, « From ranking algorithms to "ranking cultures": Investigating the modulation of visibility in YouTube search results », *Convergence*, vol. 24, p. 50-68

au nombre de vidéos publiées par des chaînes YouTube très productives, ce qui amène les vidéos publiées par des propagandistes actifs de YouTube à être mieux classées que des vidéos pourtant plus vues, plus explicatives et/ou provenant de médias traditionnels. Pour la requête [gamergate] – le Gamergate était une campagne de cyberharcèlement contre des programmeuses de jeux vidéo et féministes –, les vidéos de l'*alt-right* (droite antisystème) occupent les premières places du classement, tandis que la vidéo explicative d'une victime de cette campagne cumulait le plus grand nombre de vues mais ne se hissait pas au-dessus de la 14^e place du classement, et les vidéos publiées par les médias traditionnels exposant les interviews des victimes sont relégués tout en bas du classement.

Le nombre de vues et le nombre de commentaires suscités par une vidéo ne semblent pas des critères déterminants de classement, quelle que soit la recherche effectuée sur YouTube. Les chercheurs en concluent que « *la fonction de recherche de YouTube est très réactive aux cycles d'attention* » et que les contenus natifs de YouTube prédominent le classement. « *Des cas comme (...) la requête [495yrie] et la présence générale de personnalités YouTube souvent de droite ou d'extrême droite montrent que la plateforme vidéo organise le classement des recherches de manière à permettre aux « entrepreneurs de niche » très actifs d'obtenir des niveaux exceptionnels de visibilité. Se nourrissant de controverses et de publics fidèles, ces chaînes apparaissent systématiquement en première position, même si leurs vidéos reçoivent le plus souvent moins de vues que des voix plus traditionnelles ou conciliantes. Contrairement à l'idée que de simples mesures de popularité et la recherche du plus petit dénominateur commun stimulent la visibilité en ligne, nous avons pu avoir un aperçu des cultures de classement complexes qui récompensent les stratégies spécifiques à la plateforme et l'activation de l'audience grâce à une expression fortement opiniâtre.* ». En somme, contrairement à une idée reçue, la surexposition algorithmique par YouTube ne résulte pas simplement de la popularité d'une vidéo (nombre de vues), ni même des réactions qu'elle provoque (commentaires), mais de l'audience que peut susciter la vidéo (potentialité évaluée notamment par le nombre de recherches renvoyant à cette vidéo, par la productivité d'un vidéaste YouTube, par le fait que la vidéo provienne originellement de YouTube, par l'actualité à laquelle la vidéo fait écho...). Or, en présence de sujets controversés, les auteurs de l'étude démontrent que ces règles algorithmiques privilégiaient dans de nombreux cas en 2018 la surexposition de vidéos propagandistes, haineuses voire de désinformation plutôt que la surexposition de vidéos publiées par des médias fiables, de vidéos explicatives et de vidéos conciliantes (pourtant plus vues).

Outre l'algorithme de recommandations de YouTube, on prend celui de Twitter pour deuxième exemple. Depuis qu'Elon Musk a rendu publique une partie de l'algorithme de recommandations de Twitter le 31 mars 2023, on sait que la portée d'un tweet est amplifiée par le nombre de likes, de retweets et de réponses dont il bénéficie, qu'elle est aussi amplifiée si le tweet contient des images ou des vidéos et si l'auteur du tweet paie un abonnement Twitter Blue, mais qu'elle est au contraire réduite si l'auteur du tweet est bloqué ou si le tweet est masqué ou signalé par un grand nombre d'utilisateurs¹²⁶⁹. Sont ainsi surexposés les tweets qui peuvent susciter de l'audience (présence d'images ou de vidéos, nombre de likes et de retweets...) ou des réactions (nombre de réponses). Or, une étude publiée en mai 2023 démontre que l'algorithme de

¹²⁶⁹ LELLOUCHE Nicolas, « Les secrets de l'algorithme de Twitter rendus publics : voici ce qu'on apprend » [en ligne], *Numerama*, 3 avr. 2023

Twitter amplifie lui aussi la portée des contenus haineux¹²⁷⁰. Cette enquête, qui repose sur 806 participants, s'appuie sur deux jeux de données : les dix premiers tweets que l'algorithme leur a montrés (classement personnalisé, choisi par l'algorithme) ; et les dix premiers tweets que les utilisateurs auraient vus si Twitter leur avait montré les derniers tweets publiés par les personnes qu'ils suivent (classement chronologique, non choisi par l'algorithme). Les chercheurs constatent d'abord que les tweets proposés par le classement personnalisé sont plus relayés par les participants que les tweets proposés par le classement chronologique (16 302 tweets likés pour le classement personnalisé contre 2 232 pour le classement chronologique, 1 884 retweets contre 363). Cela signifie que l'algorithme de Twitter réussit effectivement à promouvoir des contenus qui ont une forte propension à l'audience.

Les chercheurs interrogent ensuite les participants à l'étude sur leur groupe politique d'appartenance (avec cinq choix, allant de « Extrême droite » à « Extrême gauche »), sur l'animosité exprimée par les tweets à l'encontre d'un groupe extérieur au groupe d'appartenance (« Le tweet de [@utilisateur-untel] exprime-t-il de la colère, de la frustration ou de l'hostilité envers une personne ou un groupe [le groupe politique extérieur de l'auteur = gauche/droite] ? »), sur les émotions exprimées par les tweets (anxiété, joie, tristesse et colère) et sur les émotions ressenties par les participants à la lecture de ces tweets (mêmes émotions testées). Ils constatent que, par rapport au classement chronologique, l'algorithme amplifie principalement les tweets colériques (écart-type de +40% avec le classement chronologique), puis les tweets tristes (écart-type de +22%), les tweets anxieux (écart-type de +21%) et enfin les tweets joyeux (+12%). Ils observent par ailleurs que la colère est l'émotion la plus ressentie par les lecteurs de ces tweets (écart-type de +22%), devant la joie (écart-type de +12%), l'anxiété (+11%) et la tristesse (+10%). Par rapport aux tweets à caractère politique que propose le classement chronologique, l'algorithme amplifie très fortement les tweets politiques qui expriment de la colère (écart-type de +64%), devant la tristesse (+24%), l'anxiété (+10,8%) et la joie (+2,9%). La colère domine aussi les émotions des lecteurs de tweets politiques proposés par l'algorithme (écart-type de +31% avec les tweets politiques du classement chronologique, devant la joie à +7%). Les auteurs de l'étude en concluent que « *l'algorithme peut contribuer à la polarisation affective (...), c'est-à-dire la tendance des partisans à ne pas aimer et à se méfier des personnes de l'autre camp, [indépendamment] de toute bulle de filtres*¹²⁷¹. (...) Après avoir lu les tweets sélectionnés par l'algorithme, les utilisateurs ont tendance à avoir des perceptions plus positives de leur groupe d'appartenance et plus négatives de leur groupe extérieur que

¹²⁷⁰ MILLI Smitha, CARROLL Micah, SASHRIKA Pandey, WANG Yike et DRAGAN Anca D., « Twitter's Algorithm: Amplifying Anger, Animosity, and Affective Polarization », *ArXiv*, 26 mai 2023

¹²⁷¹ La « bulle de filtres » est une intuition politique et non-scientifique émise par le militant Eli Pariser en 2011, selon laquelle les algorithmes enfermeraient les utilisateurs dans leurs propres centres d'intérêt, les privant ainsi de découvrir des informations étrangères à leurs centres d'intérêt, donc provoquant une fermeture d'esprit des utilisateurs et aggravant la polarisation. De nombreux chercheurs ont expérimenté cette théorie, sans trouver l'existence de preuves scientifiques d'une bulle de filtres polarisante, et ont au contraire trouvé la preuve qu'une exposition de l'utilisateur à des points de vue hautement contraires aux siens peut aggraver la polarisation : GUESS Andrew, NYHAN Brendan, LYONS Benjamin et REIFLER Jason, « Avoiding the echo chamber about echo chambers », *Knight Foundation*, vol. 2, 2018, p. 1–25 ; BAIL Christopher A., ARGYLE Lisa P., BROWN Taylor W., BUMPUS John P., CHEN Haochan, HUNZAKER Fallin M.B., LEE Jaemin, MANN Marcus, MERHOUT Friedolin et VOLFOVSKY Alexander, « Exposure to opposing views on social media can increase political polarization », *Proceedings of the National Academy of Sciences*, vol. 115, 2018, p. 9216–9221 ; LEVY Ro'ee, « Social media, news consumption, and polarization: Evidence from a field experiment », *American economic review*, vol. 111, 2021, p. 831–870.

lorsqu'ils lisent les tweets du classement chronologique, ce qui pourrait conduire à une plus grande polarisation affective. ».

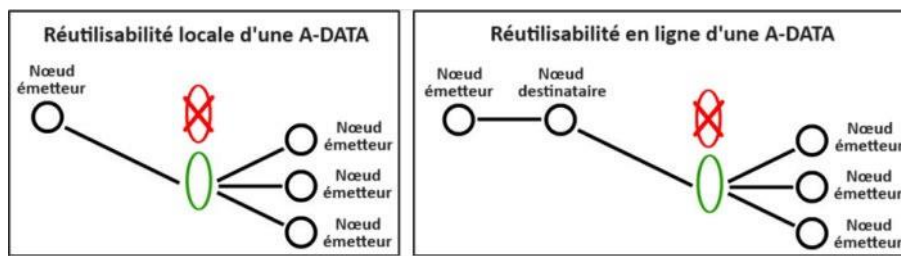
On examine enfin l'algorithme de Facebook pour dernier exemple. En 2021, la lanceuse d'alerte Frances Haugen, ex-chef de produits chez Facebook, fait fuiter des documents internes révélant que « 65% des personnes qui ont rejoint des groupes néonazis sur Facebook l'ont fait parce que l'algorithme leur avait suggéré », et que 80% des informations sur le coronavirus auraient été reçues par seulement 4% des communautés présentes sur Facebook¹²⁷². Durant son audition devant le Sénat français, elle témoigne que « l'idée [de Facebook] était de générer davantage de contenus. Quand les gens génèrent plus de contenus, on reste plus longtemps sur le site, et on consomme plus de publicités. C'est le modèle commercial. (...) Facebook a réalisé que, plus les clics arrivaient vite, plus il y avait de colère. ». Ces révélations confirment les conclusions d'une étude du MIT sur Facebook, soumises quelques mois avant les annonces de Frances Haugen : « les modèles d'apprentissage automatique qui maximisent l'engagement favorisent (...) la controverse, la désinformation et l'extrémisme : en termes simples, les gens aiment les choses scandaleuses. Parfois, cela enflamme les tensions politiques existantes. L'exemple le plus dévastateur à ce jour est le cas de la Birmanie, où les fausses nouvelles virales et les discours de haine à l'égard de la minorité musulmane rohingya ont fait dégénérer le conflit religieux du pays en un véritable génocide. »¹²⁷³.

L'ensemble des travaux scientifiques ici recensés nous en fait tirer la conclusion suivante : dès lors que les contenus haineux ont une propension naturelle à susciter de l'audience et des réactions (hors toute intervention algorithmique, la haine est l'une des émotions si ce n'est l'émotion qui se diffuse le plus vite sur internet), les algorithmes qui récompensent la propension à l'audience et à l'engagement risquent fortement de surexposer les contenus haineux. Autrement dit, **en promouvant la propension à l'audience et/ou à l'engagement, ces algorithmes risquent d'amplifier largement l'échelle de diffusion des contenus haineux**. On l'a observé avec l'algorithme de YouTube qui, en 2018, favorisait les vidéos des Youtubeurs les plus productifs, ce qui a eu pour effet de surexposer des contenus haineux excessivement produits sur des sujets controversés (on a vu que la production de contenus haineux alimente la production de contenus haineux). On a dressé le même constat avec l'algorithme de Twitter qui, en 2023, privilégiait les contenus les plus relayés et les plus commentés, ce qui a eu pour effet de surexposer des contenus haineux dont la propension à la diffusion est naturellement très élevée (on a vu que la production de contenus haineux par un groupe haineux alimente la haine individuelle des membres de ce groupe contre un groupe extérieur, ce qui facilite l'adhésion des membres du groupe haineux à un message hostile au groupe extérieur, donc facilite les relais de ce message et la diffusion de la haine à grande échelle). On a fait le même constat pour l'algorithme de Facebook qui, en 2021, privilégiait les contenus selon l'engagement qu'ils peuvent susciter, ce qui a eu pour effet de surexposer des contenus haineux, première source de réactions des utilisateurs (on a vu que la haine est l'une des émotions qui suscite le plus de réactions). La surexposition de A-DATA peut ainsi avoir pour effet de surexposer des R-DATA (contenus haineux, désinformation...) si ces dernières s'inscrivent dans les règles de surexposition voire les exploitent.

¹²⁷² DAVID Romain, « La lanceuse d'alerte Frances Haugen auditionnée au Sénat : une plongée glaçante dans l'arrière-cuisine de Facebook » [en ligne], *Public Sénat*, 10 nov. 2021

¹²⁷³ HAO Karen, « How Facebook got addicted to spreading misinformation » [en ligne], *MIT Technology Review*, 11 mars 2021

2. La réutilisabilité d'une A-DATA



On appelle « réutilisabilité d'une A-DATA » la technique consistant à rendre exploitable un ou plusieurs fichiers informatiques licites par n'importe quelle personne qui n'en est pas la propriétaire exclusive. L'open data est une bonne illustration de l'emploi de cette technique par les États. Apparu au France et aux États-Unis, l'open data est un mouvement qui consiste, pour les services publics, à mettre à disposition les données qu'ils produisent et collectent. Depuis 2013, l'Union européenne oblige les administrations à publier en ligne certaines informations publiques (à commencer par les documents administratifs), indépendamment de leur préexistence sous format papier¹²⁷⁴. En France, les documents administratifs sont définis comme les « *documents [qui], quels que soient leur date, leur lieu de conservation, leur forme et leur support, [sont] produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités locales ainsi que par les autres personnes publiques ou privées chargées d'une telle mission* »¹²⁷⁵. L'open data combine deux techniques de régulation par augmentation. Tout d'abord, ce mouvement s'appuie sur la pluralisation de A-DATA, en démultipliant la quantité de documents administratifs accessibles sur internet. Ensuite, l'open data s'appuie sur la réutilisabilité des A-DATA. En effet, les services publics ne sont pas seulement tenus de rendre ces documents accessibles ; ils doivent les rendre réutilisables par tout un chacun, c'est-à-dire les convertir dans un format transformable et modifiable par l'utilisateur¹²⁷⁶.

Pour rester sur le cas français, la loi pour une République numérique de 2016 définit une ossature de l'open data en prévoyant cinq modalités d'ouverture des données publiques. Trois d'entre elles obligent les administrations à publier des documents administratifs : la communication (doivent être publiés les documents dont les administrés ont demandé la communication auprès de la Commission d'accès aux documents administratifs en application de la loi dite CADA du 17 juillet 1978¹²⁷⁷) ;

¹²⁷⁴ Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public. Avant cette directive, en France, l'ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques laissait aux administrations la possibilité (et non l'obligation) de rendre accessibles en ligne les documents administratifs déjà émis sous format papier.

¹²⁷⁵ Code des relation entre le public et l'administration (CRPA), art. L. 300-2

¹²⁷⁶ *Ibid.*, art. L. 300-4, issu de l'art. 3 de la loi pour une République numérique de 2016

¹²⁷⁷ Toutefois, certains documents ne sont pas communicables (art. L. 311-5 CRPA), et d'autres ne sont communicables qu'à l'intéressé (art. L. 311-6 CRPA). Ne sont pas communicables les documents préparatoires (avis du Conseil d'Etat et des juridictions administratives, documents administratifs produits ou reçus pour l'instruction de la Cour des comptes, de l'Autorité de la concurrence, les docs accréditant les établissements de santé...), et les documents dont la communication porterait atteinte aux secrets protégés par la loi (secret de la défense nationale, des délibérations du pouvoir exécutif, secret médical entre le patient et son médecin à l'hôpital public...), à la sécurité (sûreté de l'Etat/sécurité des personnes/cybersécurité des administrations, tels que des décrets non publiés

la diffusion, sous réserve que les documents aient préalablement été informatisés et qu'ils occultent les éléments restreignant leur communicabilité (doivent être diffusés certains documents qui n'ont pas fait l'objet d'une communication préalable, comme les « *principaux documents* » dans lesquels figurent les informations détenues ou produites par ces administrations, les données mises à jour dont la publication présente un intérêt économique, social, sanitaire ou environnemental, et les bases de données produites ou reçues par les administrations qui n'ont pas déjà fait l'objet d'une diffusion comme les décisions de justice)¹²⁷⁸ ; la publication de données de référence (doivent être publiées sur une plateforme unique au moins neuf jeux de données utiles aux personnes publiques et privées autres que l'administration qui les détient¹²⁷⁹). Les deux dernières modalités d'ouverture des données publiques ne concernent pas seulement des documents administratifs, et couvrent les personnes aussi bien publiques que privées : la publication des données d'intérêt général (certaines données dites d'intérêt général, limitativement énumérées par la loi pour une République numérique, doivent être mises à disposition de tous)¹²⁸⁰ ; et l'open access (tout chercheur peut, six à douze mois après la publication de son travail dans un périodique paraissant au moins une fois par an, déposer ses écrits scientifiques sur un service d'archive gratuitement accessible à tous)¹²⁸¹.

Outre l'open data, la réutilisabilité d'une A-DATA trouve d'autres formes d'expression. Un des exemples les plus connus est sans doute l'open source qui consiste, pour un programmeur, à rendre exploitable le code source de son logiciel par n'importe qui, et à lui en conférer légalement le droit au moyen de la licence du logiciel. La société Alphabet a pleinement profité de cette technique pour développer son système d'exploitation Android. Android est un système

instaurant des fichiers de souveraineté secrets ou certains communiqués de l'ANSSI à destination des administrations pour se prémunir contre un virus en cours), aux missions régaliennes (conduite de la politique extérieure de la France tels que des traités internationaux tenus pour secrets – tel le réseau ECHELON –, monnaie et crédit public, recherche et prévention d'infractions de toute nature) ou au fonctionnement de la justice (par ex., si la communication d'un document relatif à une procédure en cours compromet le bon déroulement de cette procédure). Ne sont communicables qu'à l'intéressé les documents qui portent une appréciation ou un jugement de valeur sur une personne physique nommément désignée ou facilement identifiable (par ex., une sanction professionnelle motivée par la paresse d'un fonctionnaire), qui font apparaître le comportement d'une personne dont la divulgation lui porterait préjudice (par ex., le patient d'une structure psychiatrique publique dont le dossier médical ne peut être communiqué qu'à lui) ou qui, s'ils étaient communiqués, porteraient atteinte à la vie privée (diplôme scolaire ou universitaire...) ou au secret médical dont bénéficie une personne.

¹²⁷⁸ CRPA, art. L. 312-1-1, issu de l'art. 6 de la loi pour une République numérique

¹²⁷⁹ CRPA, art. L. 321-4, issu de l'art. 14 de la loi pour une République numérique. D'après l'art. R. 321-5 CRPA, issu du décret n° 2017-331 du 14 mars 2017, les neuf jeux de données sont les suivants : la Base Adresse Nationale (BAN), qui recense les adresses postales ; les numéros SIREN et SIRET ; le Code Officiel Géographique (COG) qui recense les codes géographiques et libellés des collectivités locales et des territoires étrangers ; le Plan Cadastral Informatisé ; le Registre parcellaire graphique (RPG) qui recense le périmètre des parcelles et îlots culturels ; le Répertoire de l'organisation administrative de l'État qui recense les institutions régies par la Constitution de la Ve République et les administrations qui en dépendent, soit environ 6 000 organismes ; le Répertoire à grande échelle (RGE) qui décrit précisément l'homogénéité du territoire français et l'occupation de son sol ; le Répertoire national des associations (RNA) qui recense les associations relevant la loi du 1^{er} juillet 1901 ; et le Répertoire Opérationnel des Métiers et des Emplois (ROME) qui regroupe l'ensemble des métiers regroupés par fiches, elles-mêmes organisées par domaines professionnels.

¹²⁸⁰ Cela couvre les données produites ou collectées par les concessionnaires de délégations de service public (transports, gestion de l'eau, des déchets...) dans le cadre de leur exploitation et dans la limite de ce qui est indispensable à l'exécution du contrat de délégation, les données relatives aux subventions supérieures à 23 000€, ou encore les données de consommation d'énergie électrique (Linky...).

¹²⁸¹ Loi pour une République numérique, art. 30

d'exploitation mobile open source, ce qui permet à n'importe quel fabricant de smartphone (Samsung, Xiaomi, Huawei, BBK Electronics...) de réutiliser gratuitement ce système d'exploitation et d'en modifier le code source avant de l'implémenter à leurs téléphones. Alphabet pratique ici une réutilisabilité locale (et non en ligne) d'Android : divers noeuds émetteurs (les terminaux conçus par les fabricants) peuvent réutiliser localement les données constitutives d'Android. Ce gros avantage économique et technologique qu'Android offre aux fabricants de smartphones a conduit à l'adoption d'Android par les fabricants les plus importants dans le monde entier – excepté Apple. Insérées au système Android, les applications d'Alphabet (Chrome, Google Search, Play Store, Google Maps, YouTube, Gmail, Google Drive, Google Assistant...) se retrouvent alors présentes sur la plupart des smartphones vendus dans le monde – excepté en Chine où la majorité de ces applications est illégale.

L'open source est aussi une pratique parfois recourue par les États, comme la Chine. En 2001, le gouvernement chinois charge l'Université nationale des technologies de la défense de l'Armée populaire de développer un système d'exploitation chinois pour les ordinateurs de gouvernementaux et militaires : le système d'exploitation Kylin. Cette initiative étatique semble avoir d'abord été motivée par la volonté de préserver les systèmes informatique de l'armée et du gouvernement chinois en cas de cyberguerre¹²⁸². En 2010, la version 3.0 de Kylin a une nouvelle base de code (en s'appuyant sur le système d'exploitation open source Linux et non plus sur FreeBSD), et s'étend aux secteurs importants de l'économie chinoise (énergie...) en sus de l'armée et du gouvernement¹²⁸³. En 2022, le gouvernement lance une version open source de son système d'exploitation, baptisée *openKylin* et ouverte au grand public¹²⁸⁴.

Tout aussi connus que l'open source, les wikis sont un autre exemple de A-DATA réutilisables. Un wiki a pour principe de fonctionnement de fournir aux internautes un contenu modifiable par n'importe quel utilisateur en qualité de contributeur. Wikipédia, Fandom, WikiHow ou encore Baidu Baïke sont des wikis. En plus, de l'open data, de l'open source et des wikis, on prend un quatrième exemple de réutilisabilité de A-DATA : la mise à disposition gratuite par les applications de leur API (*Application Programming Interface*). Une API est l'interface logicielle d'une application grâce à laquelle un programmeur tiers peut développer des applications interopérables avec l'application dont l'API est réutilisable. En d'autres termes, l'API est l'interface d'une application qui permet à des programmeurs tiers de construire, sur cette application, leurs propres applications. Par exemple, sur Twitter, un grand nombre de comptes utilisateurs automatisés (bots) produisent des messages chaque fois qu'ils sont mentionnés par d'autres utilisateurs : le compte @DownVideoBot répond à l'utilisateur qui le mentionne sous un tweet en renvoyant vers un hyperlien pour télécharger la vidéo contenue dans le tweet ; le compte @Colorize_bot répond à l'utilisateur qui le mentionne sous un tweet en produisant une version colorisée par IA de l'image en noir et blanc contenue dans le tweet ; le compte @RemindMe_OfThis rappelle à l'utilisateur qui le mentionne sous un tweet l'existence de ce tweet dans le délai défini par l'utilisateur, de façon à ce que ce dernier puisse

¹²⁸² C'est du moins la motivation à laquelle conclut un rapport présenté à la Commission États-Unis/Chin pour l'Économie et la Sécurité : GERTZ Bill, « China blocks U.S. from cyber warfare », *The Washington Times*, 12 mai 2009

¹²⁸³ KAN Michael, « China OS Makers Partner on New Operating System Brand », *PCWorld*, 20 déc. 2010

¹²⁸⁴ « Pour réduire sa dépendance à Windows et macOS, la Chine travaille sur son propre système d'exploitation », *01net*, 4 juil. 2022

se réserver pour plus tard la lecture ou une réponse à ce tweet etc. Tous ces comptes automatisés sont des logiciels créés grâce à l'API de Twitter, donc interopérables avec Twitter. Ils permettent d'augmenter les fonctionnalités disponibles sur Twitter – télécharger les vidéos publiées sur Twitter, coloriser des photos en noir et blanc, se faire rappeler certains tweets...

On reconnaît deux principaux avantages à la réutilisabilité d'une A-DATA. Premier avantage : **la réutilisabilité d'une A-DATA facilite la diffusion de cette A-DATA**. En effet, la réutilisabilité d'une A-DATA consiste précisément à ouvrir la possibilité que des relais diffusent cette A-DATA : les ré-utilisateurs, *i.e.* les personnes (fabricants, programmeurs, internautes...) autorisées à modifier et à rediffuser les fichiers informatiques de la A-DATA sans en être les propriétaires exclusifs. Plus les ré-utilisateurs sont des prescripteurs numériques centraux (par ex. les principaux fabricants de smartphones), plus la A-DATA réutilisée (par ex. un système d'exploitation mobile) peut voir son échelle de diffusion être amplifiée.

Concrètement, dans le cas de l'open data, les A-DATA réutilisables sont les documents administratifs et informations publiques ; la réutilisabilité des documents administratifs et informations publiques facilite la diffusion sur internet de ces documents et informations (par des journalistes, chercheurs, utilisateurs avertis... qui s'en feront le relai). De même, dans le cas de l'open source, la A-DATA réutilisable est le logiciel librement exploitable (par ex. le système d'exploitation Android) ; la réutilisabilité du logiciel libre facilite la diffusion sur internet de ce logiciel (par les fabricants de smartphones qui s'en sont faits les relais). Ou encore, dans le cas des API, la A-DATA réutilisable est l'interface de l'application principale (par ex. Twitter) ; la réutilisabilité de l'API facilite la diffusion sur internet de cette interface (par les programmeurs tiers qui s'en font les relais).

Deuxième avantage : **la réutilisabilité d'une A-DATA améliore la qualité de la A-DATA au fil des contributions et réutilisations**. En effet, les ré-utilisateurs peuvent diffuser une A-DATA en lui apportant une valeur ajoutée : les chercheurs peuvent découvrir et partager des conclusions scientifiques en réutilisant les documents administratifs et informations publiques accessibles ; les programmeurs peuvent réutiliser un logiciel open source pour corriger ses failles de sécurité, augmenter les fonctionnalités disponibles, ou encore offrir un design plus recherché par la demande. De même, les applications tierces construites sur l'API d'une application principale permettent d'enrichir l'application principale, comme on l'a observé avec Twitter.

Le réseau social Reddit est un autre exemple illustratif de la qualité apportée par la réutilisabilité de l'API. En 2017, le programmeur Christian Selig créé Apollo for Reddit, une application construite sur l'API de Reddit et compatible avec iOS. Téléchargeable sur les magasins d'applications (Play Store, AppStore...), Apollo for Reddit permettait aux utilisateurs d'iPhones d'accéder à une version de Reddit masquant les publicités et les messages de la modération automatisée de Reddit (AutoModerator), mettant en évidence les nouveaux comptes utilisateurs (pour repérer les trolls qui démultiplient le nombre de nouveaux comptes), adaptant le design de Reddit aux commandes gestuelles d'Apple, et proposant aux utilisateurs de s'occuper d'un petit animal de compagnie pixellisé en 2D de type Tamagotchi. En plus d'Apollo, de nombreuses autres applications tierces ont été érigées sur l'API de Reddit, telles que : rif is fun for Reddit (équivalent d'Apollo pour les utilisateurs d'Android) ; SYNC (qui propose un design très épuré et pratique de Reddit, affichant chaque contenu sous la forme d'une vignette/carte pour permettre à l'utilisateur d'avoir un aperçu rapide de son fil, facilitant le passage d'un commentaire à un autre sans devoir faire défiler toutes les réponses au premier commentaire, facilitant le retour au fil d'actualité principal depuis la section commentaires, facilitant l'accès aux subreddits depuis le fil principal, donnant à l'utilisateur la possibilité de personnaliser les subreddits

ou groupes de subreddits qui s'affichent dans son fil...) ; ReddPlanet (qui permet de personnaliser le design de Reddit selon les préférences de l'utilisateur, par ex. en affichant les articles en mode normal ou plein écran, en modifiant le thème d'affichage, en faisant varier l'emplacement du menus et des options etc.)...

En février 2023, Twitter rend payante toute réutilisation de son API et, en avril 2023, Reddit annonce à son tour la fin de la gratuité pour la réutilisation de son API. Le 31 mai 2023, Reddit fait connaître les prix d'accès à son API. À la même date, Christian Selig fait part de la difficulté à payer les prix fixés. Le 8 juin, il ferme son application Apollo utilisée par 1,3 à 1,5 millions d'internautes. Le lendemain, rif (3 à 5 millions d'utilisateurs), Sync (1 million d'utilisateurs) et ReddPlanet annoncent qu'elles fermeront toutes trois le 30 juin, pour les mêmes raisons qu'Apollo¹²⁸⁵. Ces fermetures d'applications tierces populaires ont déclenché une vague de protestation des utilisateurs de Reddit contre la décision de l'entreprise de rendre l'API payante. Les modérateurs de Reddit – des utilisateurs bénévoles qui administrent les subreddits – évoquent une « grève » et ferment près de 9 000 subreddits entre les 12 et 17 juin, soit 5 à 8% de la totalité des communautés Reddit (i.e. 5 à 8% des subreddits actifs)¹²⁸⁶. Cinq des dix subreddits les plus populaires ont fermé – r/gaming (38 millions d'abonnés), r/aww (34,5 millions d'abonnés), r/Music (32,9 millions d'abonnés), r/todayilearned (32,8 millions d'abonnés) et r/pics (30 millions d'abonnés)¹²⁸⁷. La grève était prévue pour ne durer que 24h à 48h, mais elle a démontré une capacité à pénaliser fortement l'entreprise le temps qu'elle a duré : les fermetures massives et simultanées de subreddits ont provoqué une panne de l'application dans la matinée du 12 juin, mais ont aussi conduit à une diminution de 7% du trafic quotidien de Reddit et de 16% du temps passé par les utilisateurs sur la plateforme entre les 12 et 13 juin, ainsi qu'à une chute de 20% du nombre de visites quotidiennes sur le portail publicitaire de Reddit entre les 13 et 23 juin (probablement due au fait que les annonceurs étaient moins disposés à faire affaire avec le réseau social)¹²⁸⁸. Les protestations sur Reddit sont révélatrices de l'avantage qualitatif que les applications tierces apportent à Reddit : des millions d'utilisateurs y ont vu un intérêt tel que les priver de ces applications a provoqué un mouvement de contestation d'une très grande ampleur. Comme pour l'open source et l'open data, la réutilisabilité d'une API enrichit la qualité de la A-DATA réutilisée (l'interface de Reddit en l'espèce).

Inversement, on reconnaît deux principaux inconvénients à la réutilisabilité d'une A-DATA. Premier inconvénient : **la réutilisabilité d'une A-DATA s'accompagne d'un risque élevé de délaissement**. En effet, les ré-utilisateurs potentiels ont la liberté d'accéder ou non à la A-DATA réutilisable. Concrètement, les ré-utilisateurs peuvent très bien délaisser les informations publiques mises en ligne par open data, délaisser des logiciels open source licites, délaisser un wiki ou délaisser une API. On a vu que ce risque peut être relativisé de plusieurs manières – par surexposition d'une A-DATA, ou si l'offre légale satisfait la demande. Deuxième inconvénient : **la réutilisabilité d'une A-DATA peut être exploitée pour produire une R-DATA**. En effet, si une A-DATA est réutilisable par n'importe qui, il n'est par définition

¹²⁸⁵ PETERS Jay, « It's not just Apollo: other Reddit apps are shutting down, too », *The Verge*, 9 juin 2023

¹²⁸⁶ PETERS J., « 8,471 subreddits have gone dark », *The Verge*, 13 juin 2023 ; PHILIPS-GRANTHAM Wyatte, « Reddit CEO defiant as moderator strike shuts thousands of forums: 'We made a business decision that we're not negotiating on' », *Fortune*, 17 juin 2023

¹²⁸⁷ GERKEN Tom, « Reddit blackout: Subreddits to go private on Monday », *BBC*, 9 juin 2023

¹²⁸⁸ PEREZ Luna, « Apollo, Relay, Rif is fun : quelles apps alternatives pour accéder à Reddit ? », *Numerama*, 13 juin 2023 ; SINGH Jagmeet, « Reddit protest plunges user engagement, site activity and ad portal visits », *TechCrunch*, 28 juin 2023

pas possible de contrôler les réutilisations qui en sont faites. Par exemple, un logiciel open source rend public son code source, ce qui permet à un cyberattaquant de connaître les failles du code du logiciel. Le cyberattaquant peut aussi reproduire le code source du logiciel pour créer un logiciel clone qui contient du code malveillant. De même, un groupe terroriste peut s'appuyer sur les données françaises cadastrales, géographiques et institutionnelles mises en open data pour préparer un attentat en France. Ou encore, des contributeurs de Wikipédia peuvent diffuser sur l'encyclopédie en ligne des propos diffamatoires, des injures, des fausses informations¹²⁸⁹ ...

On récapitule ci-haut les diverses configurations des techniques de régulation étudiées. Nous n'avons malheureusement ni le temps, ni l'espace pour étudier toutes les techniques de régulation. Certaines n'ont donc pas été abordées comme : le transfert d'une A-DATA (technique d'augmentation consistant à transférer les fichiers informatiques constitutifs d'une A-DATA depuis la machine qui les hébergeait vers une autre machine)¹²⁹⁰ ; la sous-exposition de R-DATA (technique de restriction consistant à réduire la visibilité d'une R-DATA)¹²⁹¹ ; ou encore la surveillance des données produites et/ou stockées (technique qui ne s'applique ni à augmenter, ni à restreindre l'accès à une A-DATA ou à une R-DATA, mais qui consiste à employer des logiciels de surveillance des données stockées localement ou diffusées en ligne). Cependant, on a étudié un échantillon de 15 techniques de régulation qui nous semble suffisant pour pouvoir expérimenter l'efficacité de l'action régulatrice sur internet (Section 2).

Section 2. Théorisation de l'efficacité de la régulation du cyberspace

Pour finir, on théoriserait l'efficacité de la régulation du cyberspace : en modélisant les configurations de contournement dans lesquelles peuvent s'inscrire les prescripteurs numériques (Paragraphe 1) ; et en proposant un modèle théorique censé permettre le contrôle de l'échelle de diffusion d'une donnée dans le cyberspace (Paragraphe 2).

Paragraphe 1 – Les configurations de contournement

On décortiquera les configurations de contournement en trois catégories : celles qui ne s'appuient pas sur un intermédiaire (A) ; celles qui s'appuient sur un intermédiaire au moins (B) ; et celles qui sont pratiquées à l'aide d'un périphérique accessoire (C).

¹²⁸⁹ En 2008, le juge français de première instance a prescrit à Wikipédia de communiquer au requérant l'adresse IP du contributeur qui a publié des propos diffamatoires et injurieux (« *gros con, grosse merde* ») sur un article de l'encyclopédie en ligne : Tribunal de grande instance de Nanterre, Juge des référés, 10 juillet 2008, n° 08/01490, cité par DIMEGLIO Arnaud et LY TONG PAO Nakita « La responsabilité de Wikipédia », *Village de la Justice*, 26 juin 2019

¹²⁹⁰ Un exemple du recours par les États à la technique du transfert de A-DATA réside dans le droit à la portabilité des données, qui permet à l'utilisateur d'exiger au responsable de traitement de transférer ses données vers un autre responsable de traitement, voire vers le terminal de l'utilisateur directement

¹²⁹¹ Il en va ainsi de Google Search, qui déclassé certains résultats jugés problématiques, *i.e.* qui renvoie ces résultats en fin de classement : PONCET Gueric, « Google déclassé les mauvais sites », *Le Point*, 28 fév. 2011 (sites aux contenus copiés/plagiés) ; BEKY Ariane, « Google déclassé des sites "pirates" à l'échelle mondiale », sur *Silicon.fr*, 21 oct. 2014 ; « Google : Les sites trop lents sur mobile seront déclassés », *20 Minutes*, 19 janv. 2018 ; GALTIER-FAMIÉ Héloïse, « Pénalités Google : comment les détecter et comment réagir », *Blog du Modérateur*, 31 août 2021

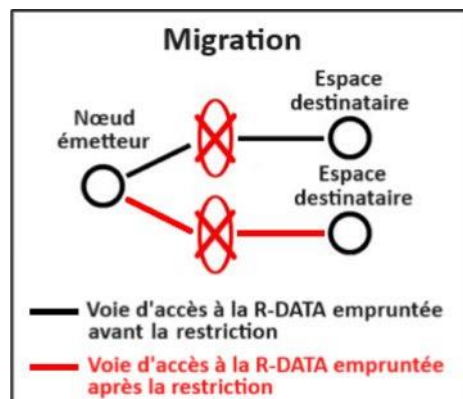
A) Les configurations de contournement qui ne reposent pas sur des intermédiaires

1. La migration

Le concept de « contournement » renvoie à une diversité de configurations. En d'autres termes, un prescripteur numérique peut contourner une technique de régulation de différentes manières. On rapporte ici les configurations qu'on a identifiées.

Sera d'abord traitée la configuration de la migration. On appelle « migration » la configuration dans laquelle un prescripteur cesse de faire exécuter ses requêtes dans un espace logique, pour les faire exécuter dans un autre espace logique¹²⁹². La migration peut être employée afin de contourner la restriction d'accès à une R-DATA. Dans ce cas, la migration se concrétise ainsi (ci-contre) : avant la restriction, le prescripteur numérique accédait à une R-DATA qui était exécutée dans un espace logique ; après la restriction de l'accès à cette R-DATA par cet espace logique, le prescripteur persiste à produire la même R-DATA en choisissant un autre espace logique qui n'applique pas ou ne se voit pas

appliquée la restriction. Par exemple, si est restreint l'accès à une application de consommation illicite de films, les utilisateurs peuvent migrer vers une autre application de consommation illicite de films dont l'accès n'est pas restreint.



Cette configuration est identifiée de longue date. On a vu que, en 1997, David Post et David Johnson considéraient même la migration comme la seule option dont disposaient les utilisateurs pour fuir une application qui plonge dans « *l'anarchie* »¹²⁹³. Il est par ailleurs courant de lire dans la presse que les utilisateurs de telle application ou de tel système d'exploitation ont « migré » vers telle autre application ou système d'exploitation¹²⁹⁴.

¹²⁹² On rappelle avoir défini l'« espace logique » comme un espace mémoire virtuel (i.e. simulé par un logiciel, comme un segment ou une page mémoire ; la quasi-totalité des machines numériques est aujourd'hui équipée d'une mémoire virtuelle). Toute personne qui souhaite accéder à des données doit accéder à l'espace mémoire qui stocke ces données, donc la production de toute requête nécessite d'accéder à un espace logique. Par exemple, l'utilisateur qui souhaite accéder à son système d'exploitation doit accéder à la partie de l'espace mémoire logique de sa machine qui stocke ce système pour en ordonner l'exécution ; celui qui souhaite accéder à une application en ligne doit accéder à la partie de l'espace mémoire du serveur qui héberge cette application etc. Par opposition, l'espace mémoire physique désigne les espaces mémoires de la machine qui dépendent de ses composants physiques (espaces appelés « cases », insuffisantes pour stocker toutes les données, et sur lesquelles se superposent les pages et segments virtuels). La somme de tous les espaces logiques connectés à internet forme ce qu'on appelle le « cyberspace ».

¹²⁹³ JOHNSON David et POST David, « And How Shall the Net be Governed ? » in KAHIN B. et KELLER J. H. (dir.), *Coordinating the Internet*, préc., 1997

¹²⁹⁴ WALLIN Jack, « Dix manières d'aider les utilisateurs à migrer de Microsoft Office vers LibreOffice », *ZDNet*, 12 fév. 2015 ; CAULIER Sophie, « Numérique : le cloud, enjeu de souveraineté », *Le Monde*, 16 fév. 2020 (« beaucoup d'entreprises migrent vers AWS ou Azure, les clouds d'Amazon et de Microsoft, car ces grands acteurs américains ont énormément investi et créent sans arrêt de nouvelles fonctionnalités qui apportent de l'innovation et donc de la performance ») ; «

On détaillera ici l'exemple des *alt-tech*, c'est-à-dire des applications principalement fréquentées par la droite alternative américaine, par la droite complotiste, par l'extrême droite et par la droite conservatrice. Au début des années 2020, des migrations massives ont été constatées de la part de ces utilisateurs radicaux pour contourner les restrictions d'accès les ayant frappé. Deux événements ont été à l'origine de ce vaste mouvement migratoire : les restrictions de l'accès à Parler, un réseau social qui avait une philosophie très laxiste de censure des contenus haineux (notamment racistes, misogynes, homophobes...) ; et le bannissement des comptes de Donald Trump par les réseaux sociaux les plus populaires.

En octobre 2020, Parler ne comptait encore qu'un demi-million d'utilisateurs actifs. L'élection présidentielle américaine débute le 3 novembre 2020, lorsque les citoyens des États-Unis élisent leurs grands électeurs, et se clôture le 14 décembre 2020, lorsque les grands électeurs élisent les président et vice-président des États-Unis. Le nombre d'utilisateurs actifs de Parler connaît une hausse soudaine dans ce contexte électoral, passant de 500 000 utilisateurs (3 novembre) à 800 000 (4 novembre), puis à 1,4 millions (5 novembre), 1,9 millions (6 novembre), 2,3 millions (7 novembre) pour atteindre plus de 4 millions le 14 novembre¹²⁹⁵. La première semaine de janvier 2021, le réseau social se hisse en tête des téléchargements sur l'App Store, et Parler totalisait 9 à 13 millions d'utilisateurs actifs durant le mois de janvier¹²⁹⁶.

Le 6 janvier, le Capitole des États-Unis est envahi par des milliers d'opposants à l'élection de Joe Biden, parfois avec violence. Entre le 7 et le 13 janvier, après que le président Donald Trump ait soutenu voire encouragé les émeutiers, ses comptes sur les réseaux sociaux sont définitivement suspendus par Facebook, Instagram, Snapchat, Twitch, Twitter et YouTube. Parler est accusé de ne pas avoir agi contre les messages publiés par lesquels s'organisaient les émeutiers. Pour cette raison, Alphabet retire l'application de son Play Store le 8 janvier puis, le 9 janvier, Apple la retire à son tour de l'App Store¹²⁹⁷. Le 10 janvier, Amazon Web Services (dont les serveurs *cloud* hébergeaient Parler) suspend l'hébergement du réseau social par ses serveurs¹²⁹⁸.

Les techniques de restriction ici employées ont été des suppressions de données – à savoir la suppression des fichiers constitutifs du réseau social Parler depuis les magasins d'application Play Store et AppStore, et depuis les serveurs d'AWS. Face à ces restrictions, le nombre d'utilisateurs de Parler décline pour s'établir à 4,3 millions en février 2021, puis à 3,3 millions (mars 2021), 2,2 millions (avril 2021), 1,4 million (juin 2021), 874 000 (juillet 2021) et 496 000 (juillet

WhatsApp : de nombreux utilisateurs migrent vers Signal et Telegram », *La Dépêche*, 13 janv. 2021 ; ROCHEFORT Mathilde, « La migration d'utilisateurs de Twitter vers Mastodon est-elle vraiment significative ? », *Clubic*, 8 nov. 2022

¹²⁹⁵ RODRIGUEZ Salvador, « The four latest contenders to Facebook's social media throne », *CNBC*, 14 nov. 2020 ; DISHMAN Lydia, « Conservative playgrounds Parler and MeWe are not sustaining their pre-election growth », *Fast Company*, 7 déc. 2020

¹²⁹⁶ Entre le 3 novembre 2020 et la première semaine de janvier 2021, Parler a vu la création de 8,5 millions de nouveaux comptes utilisateurs : THIEL David, DIRESTA Renée, GROSSMAN Shelby et CRYST Elena, « Contours and Controversies of Parler », *Stanford Internet Observatory*, 28 janv. 2021, p. 13

¹²⁹⁷ « Le site web du réseau social Parler hors ligne », *Ouest-France*, 11 janv. 2021

¹²⁹⁸ « Après Google et Apple, Amazon suspend le réseau conservateur Parler », *France 24*, 10 janv. 2021

2022, soit son niveau pré-électoral de 2020)¹²⁹⁹. L'efficacité de ces restrictions est toutefois nettement entravée par une migration remarquable.

Entre les 7 et 14 janvier 2021, après la censure de Parler, le réseau social Gab (qui partage la philosophie de Parler sur la modération des contenus) gagne 2,3 millions de nouveaux utilisateurs, un chiffre colossal sur moins d'une semaine¹³⁰⁰. Le réseau social Wimkin (même philosophie) voit subitement croître son nombre d'utilisateurs jusqu'au 12 janvier, date à laquelle il est à son tour retiré de l'App Store¹³⁰¹. Le week-end des 9 et 10 janvier, le réseau social MeWe (même philosophie) gagne 400 000 nouveaux utilisateurs, et le nombre de téléchargements de la plateforme vidéo Rumble (alternative minimalement censurée de YouTube) est multiplié par 10 avec 162 000 téléchargements sur seulement deux jours¹³⁰². Quand on observe la courbe d'évolution du nombre d'utilisateurs actifs des principales alt-tech, on constate que la chute du nombre d'utilisateurs actifs de Parler entre le dernier trimestre 2020 et le premier trimestre 2021 (-9 millions) a été largement compensée par la hausse du nombre d'utilisateurs de Rumble (+12 millions), de Gab (+3,5 millions) et de MeWe (+ 1 million) sur la même période¹³⁰³.

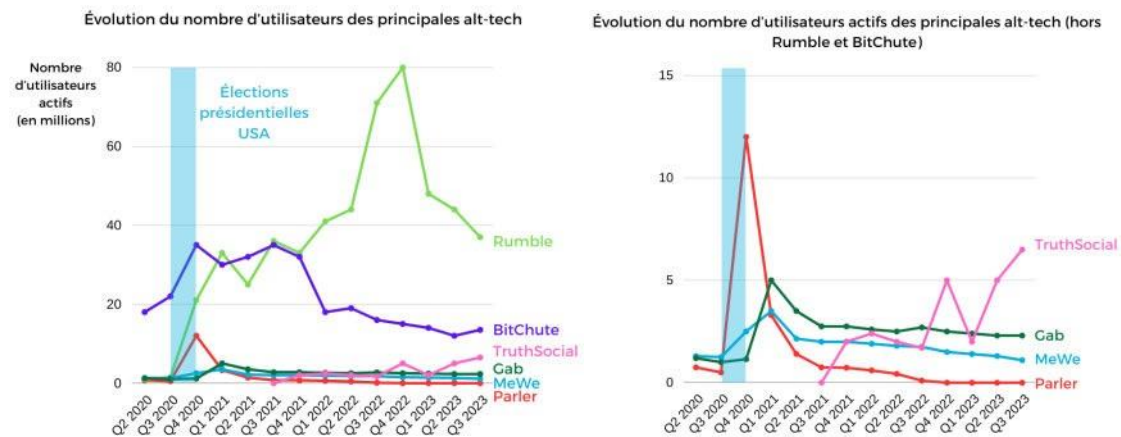
¹²⁹⁹ « Average unique monthly visitors to Parler in the United States from January to August 2021 and 2022 », *Statista*, 14 déc. 2022

¹³⁰⁰ GOODWIN Jazmin, « Gab: Everything you need to know about the fast-growing, controversial social network », *CNN Business*, 17 janv. 2021

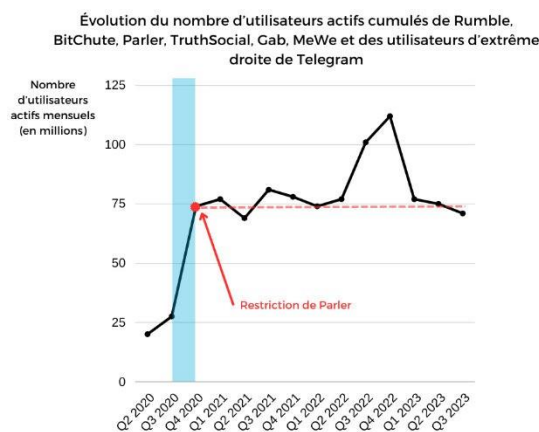
¹³⁰¹ UBERTI David, « Apple's App Store Removes Social Media Platform Wimkin Over Calls to Violence », *The Wall Street Journal*, 14 janv. 2021

¹³⁰² ABRIL Danielle, « Trump supporters flock to MeWe, Gab, and Rumble after Parler goes offline », *Fortune*, 12 janv. 2021

¹³⁰³ Pour réaliser les courbes ci-dessous, on s'est appuyé : (i) sur les données de trafic de chacune de ces applications durant toute la période observée (sources : Semrush et SimilarWeb, on a pu récupérer les données trop anciennes sur la Wayback Machine d'Internet Archive) ; (ii) sur les chiffres déclarés par les propriétaires des applications concernées (par exemple, pour Rumble, v. « Number of monthly active Rumble users worldwide from 3rd quarter 2020 to 2nd quarter 2023 », *Statista*, 28 août 2023, pour Gab v. Gab, « Annual Report », sur *Sec.gov*, 27 mai 2020, pour Parler v. RODRIGUEZ S., « The four latest contenders to Facebook's social media throne », préc., *CNBC*, nov. 2020, ou encore pour MeWe v. MURPHY Coral, « Facebook rival MeWe gains 2.5M members in a week as users seek privacy », *USA Today*, 20 janv. 2021) ; (iii) sur des articles scientifiques (par exemple, pour BitChute, on a croisé les données de trafic avec le nombre de visionnages mensuels de vidéos sur cette plateforme vidéo recensés par TRUJILLO Milo Z., GRUPPI Maurício, BUNTAIN Cody et HORNE Benjamin D., « The MeLa BitChute Dataset », *ArXiv*, 10 fév. 2022, p. 5, ou encore pour Parler v. THIEL D., DIRESTA R., GROSSMAN S. et CRYST E., « Contours and Controversies of Parler », *Stanford Internet Observatory*, préc., janv. 2021, p. 13) ; (iv) sur des enquêtes d'opinion évaluant le nombre d'utilisateurs américains réguliers de ces applications (ST. AUBIN Christopher et STOCKING Galen, « Key facts about Gab », *Pew Research Center*, 24 janv. 2023) ; et (v) sur des enquêtes d'organismes privés spécialisés (par exemple l'enquête d'AppTopia sur MeWe et Parler entre novembre et décembre 2020, v. DISHMAN Lydia, « Conservative playgrounds Parler and MeWe are not sustaining their pre-election growth », *Fast Company*, 7 déc. 2020, ou encore l'enquête en coopération avec Righting concernant le nombre d'utilisateurs de Parler, v. « Average unique monthly visitors to Parler in the United States from January to August 2021 and 2022 », *Statista*, 14 déc. 2022)



Bien que la restriction de Parler a profité à Rumble, Gab et MeWe à court terme, elle semble avoir alternativement profité à Rumble et BitChute (une autre alternative à YouTube) à moyen terme. À plus long terme, Rumble et TruthSocial (le réseau social fondé par Donald Trump en février 2022) semblent les principaux nouveaux bénéficiaires de la popularité des alt-tech. Par ailleurs, en cumulant les bases d'utilisateurs de Rumble, BitChute, Parler, TruthSocial, Gab et MeWe, ainsi que la base d'utilisateurs de Telegram identifiés d'extrême droite aux États-Unis¹³⁰⁴, on obtient la courbe suivante :



Cette courbe est obtenue par une simple addition des bases d'utilisateurs des applications concernées, et ne tient donc pas compte des doublons (nombre de personnes qui utilisent simultanément plusieurs de ces applications). On remarque que le niveau atteint juste avant la restriction de Parler (Q4 2020) a été presque constamment dépassé depuis la restriction. Ces graphiques nous amènent à la conclusion suivante : **en raison des migrations vers Rumble, Gab, BitChute, Telegram et TruthSocial, les restrictions ayant frappé Parler n'ont pas montré d'effet significatif pour réduire la**

popularité des alt-tech – ni à court terme, ni à moyen terme, ni à plus long terme. On en déduit que le recours à **la migration a permis de neutraliser l'efficacité de la restriction de Parler** en janvier 2021.

¹³⁰⁴ Au troisième trimestre 2020, on estimait entre 1 et 2 millions le nombre d'utilisateurs de Telegram d'extrême droite (pour environ 5-6 millions d'utilisateurs de Telegram aux États-Unis), contre environ 8-10 millions en 2023 (27% des 30-35 millions d'utilisateurs de Telegram aux États-Unis) : ST. AUBIN Christopher et STOCKING Galen, « Key facts about Gab », préc., *Pew Research Center*, janv. 2023 ; CECI L., « Most popular mobile messaging apps in the United States as of September 2019, by monthly active users », *Statista*, 25 août 2023 ; KUNST Alexander, « Most used messenger by brand in the U.S. as of June 2023 », *Statista*, 25 août 2023. On a inclus Telegram dans la base d'utilisateurs, car un important mouvement de migration semble avoir eu lieu de la part des utilisateurs d'extrême droite vers Telegram depuis 2020 : WALTHER Samantha et MCCOY Andrew, « US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism », *Perspectives on Terrorism*, vol. 15, avr. 2021, p. 100-124 ; ROGERS Richard, « Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media », *European Journal of Communication*, vol. 35, 6 mai 2020, p. 213-229.

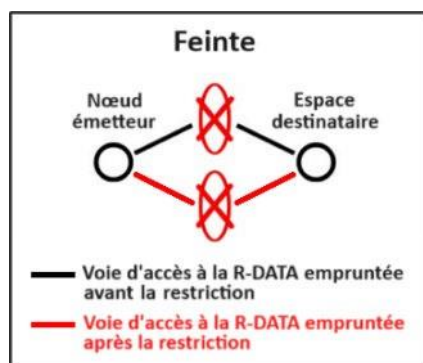
Comme toutes les techniques de contournement, la migration n'est pas l'apanage des internautes. Par définition, toute personne qui peut ordonner à la machine d'exécuter des règles – i.e. tout prescripteur numérique – peut lui ordonner d'exécuter des règles de contournement (comme la migration). Inversement, tout contournement résulte de l'exécution par la machine d'une règle qu'il lui a été ordonnée d'exécuter. Avoir identifié les catégories de prescripteurs numériques nous permet donc du même coup d'identifier les auteurs potentiels d'un contournement. Dès lors, le contournement peut être pratiqué aussi bien par les internautes que par les fabricants, les opérateurs de transmission de données, les gestionnaires d'applications, les administrateurs de serveurs et les programmeurs.

Pour rester sur la technique de la migration, cette dernière est par exemple souvent employée par les gestionnaires d'applications. Ainsi, après avoir été banni des réseaux sociaux grand public en qualité d'internaute, Donald Trump a fondé en février 2022 son propre réseau social TruthSocial. Ce faisant, il a changé d'espace logique pour persister à exprimer ses opinions. En qualité de gestionnaire d'application, Donald Trump a donc migré vers sa propre application pour contourner les restrictions qui le frappaient (en l'espèce, des blocages par bannissement). Un autre exemple fréquemment rencontré en pratique est celui des gestionnaires d'applications de consommation illicite de biens culturels (films, séries TV, retransmissions sportives en direct...). Ces applications (Wiflix, Cpasbien...) changent en effet régulièrement le TLD de leur nom de domaine (<.al>, <.io>, <.me>, <.moe>...), c'est-à-dire font migrer leur domaine vers un autre TLD pour échapper aux blocages et filtrages par noms de domaine. Recourent également à la migration les gestionnaires d'applications qui hébergent des copies conformes de leur application sur des serveurs dont l'accès n'est pas restreint (« site miroir ») : il en va ainsi de l'agence Reuters qui, en 2013, fit héberger sur un serveur étranger (le serveur d'Amazon librement accessible depuis la Chine) une copie du site web de son antenne pékinoise, ce dernier étant hébergé sur un serveur chinois qui en bloquait l'accès¹³⁰⁵. Lorsque la migration est recourue par des administrateurs d'applications, elle fournit aux utilisateurs le pouvoir de migrer à leur tour vers ces applications pour contourner la restriction.

La migration est une configuration inhérente au réseau dès lors qu'elle requiert des éléments nécessaires au fonctionnement du réseau (l'existence d'un producteur de données, et d'au moins deux espaces logiques). Pour autant, le risque de migration peut être réduit à l'aide de la centralisation. On a vu que la centralisation est une technique de régulation consistant à restreindre le nombre de voies d'accès à une donnée. Plus le réseau est centralisé, moins les utilisateurs ont donc de voies disponibles pour migrer vers un espace logique. Inversement, plus le réseau est décentralisé, plus les utilisateurs ont de choix pour migrer vers tel ou tel espace logique. Cependant, si la centralisation peut certes réduire le risque de migration, elle ne permet pas de réduire efficacement une autre configuration de contournement très populaire : la feinte.

¹³⁰⁵ CHAMPEAU Guillaume, « Amazon exploité pour contourner la censure en Chine », *Numerama*, 18 nov. 2013

2. La feinte



On appelle « feinte » la configuration de contournement dans laquelle le prescripteur persiste à produire ou stocker une R-DATA sur le même espace logique, mais en changeant la formule de production de la R-DATA. Concrètement, on a vu qu'une requête d'accès est constituée par une formule binaire, *i.e.* produite sous la forme de 0 et de 1. La feinte consiste, pour le prescripteur, à trouver une formule de production qui n'est pas restreinte afin de persister à produire ou stocker une R-DATA malgré la restriction.

On a déjà rapporté l'exemple du premier cas JVC, lorsque les internautes ont contourné la restriction des publications par mots-clés (pute, juif, pédé...) en trouvant d'autres formules non censurées (pute, ((())), pēdē...) pour persister à produire des contenus haineux. On a aussi relevé que de nombreux internautes chinois sont des fins spécialistes de la feinte, au point d'avoir développé leur propre vocabulaire anti-censure¹³⁰⁶. À cette occasion, on a constaté que la feinte a servi aux internautes chinois : pour critiquer l'action des censeurs, de l'État et du Bureau de propagande ; pour contester la politique « zéro-covid » malgré la censure ; pour contourner la censure du mouvement #MeToo ; pour diffuser des actualités censurées par l'État¹³⁰⁷...

On examine ici le cas particulier de la restriction des mouvements féministes sur internet en Chine. En février 2018, après que le gouvernement central ait ordonné aux plateformes la suppression de toutes les publications en ligne comportant les #我也是 et #米兔 (#WoYeShi, signifiant #MeToo), les partisans du mouvement Me Too se sont exprimés en mentionnant dans leurs messages les émoticônes du riz (qui se prononce *mǐ*) et du lapin (qui se prononce *tù*) ou le #MǐTù (#米兔), et des représentations audiovisuelles d'un bol de riz et d'un lapin. Au même moment, des associations et groupes féministes chinois (comptes Women's Awakening et Feminist Voices sur Weibo, groupe Hard Candy sur WeChat ...) diffusent en ligne des conseils stratégiques pour formuler des messages MeToo malgré la censure : captures d'écran immédiates d'un témoignage d'agression sexuelle, publications des textes dans un format image (long à scanner et rendant plus difficile la détection de mots sensibles par l'algorithme de censure), pivotement des textes ainsi mis en image pour empêcher la reconnaissance d'un texte par le scan algorithmique (l'inversion des caractères est très lisible pour l'être humain dans la typographie chinoise)¹³⁰⁸. En juillet 2018, le gouvernement fait censurer par les plateformes chinoises toute référence au mot « Zhu Jun » après que ce présentateur de télévision ait été accusé en ligne par six femmes de les avoir

¹³⁰⁶ « Des nouilles pho et des pandas. Comment les internautes en Chine inventent un langage pour contourner la censure liée au COVID-19 », *Amnesty International*, 6 mars 2020

¹³⁰⁷ Par exemple, en 2011, un accident de trains censuré par la Chine a été diffusé sur internet, et a suscité plus de 10 millions de critiques de la part des internautes : v. conférence TED de Jing ZHAO (Michael ANTI), « Behind the Great Firewall of China », préc., sur *Ted.com*, juin 2012

¹³⁰⁸ ZHANG Karen, « The promises and pitfalls of digital activism: Fighting for #MeToo under the Great Firewall of China », préc., *ANU Undergraduate Research Journal*, vol. 11, n° 1, avr. 2021

agressées sexuellement, mais de nombreux internautes ont à nouveau feinté la censure en utilisant le #猪菌 (#BactériesPorcines, un homophone de Zhu Jun, 朱军)¹³⁰⁹.

Le même scénario se reproduit massivement en novembre 2021. Alors que, le 2 novembre, la joueuse de tennis Peng Shuai accuse sur la plateforme Weibo l'ancien vice-premier ministre chinois Zhang Gaoli de l'avoir violée, son message est supprimé par la modération de Weibo 30 minutes après sa publication, et la plateforme censure tous les messages comportant le mot « tennis » ou mentionnant les noms de « Peng Shuai » ou « Zhang Gaoli » (le même type de censure est adopté par Douban, WeChat, QQMessage, Baidu Search... qui censurent les résultats, messages et captures d'écran afférents au sujet). Une fois de plus, les internautes se sont exprimés sur le sujet en employant des mots-clés invisibles aux algorithmes de modération comme « ps », « zgl », « Zhuge Liang » (stratège militaire historique, à la place de Zhang Gaoli), « Pu Shu », « Bodhisattva » (auteur-interprète-compositeur, à la place de Peng Shuai) ou encore « Eddie Peng est si beau » (dont le premier et le dernier mot forment le prénom de Peng Shuai)¹³¹⁰.

Avant la censure du message originel de Peng Shuai, ce message a été consulté plus de 100 000 fois sur Weibo en moins de 30 minutes et, après la censure, le nom de Peng Shuai a généré plus de 20 millions de vues sur Weibo pendant quelques heures, et le message a été recherché près de 7 millions de fois – sans compter les messages qui ont feinté la restriction à l'aide de mots-clés invisibles aux algorithmes¹³¹¹. De nombreux messages de soutien à la joueuse de tennis ont été publiés sur Weibo de la part d'utilisateurs chinois très populaires (« wanghong », 网红)¹³¹². Le lendemain de la publication, soit le 3 novembre 2021, la censure avait efficacement réduit la diffusion du message : toute référence aux accusations a disparu des réseaux sociaux chinois grand public (« les discussions en ligne étaient aussi propres qu'une feuille blanche »)¹³¹³. Compte tenu de la gravité des allégations, « les gens n'osent même pas en discuter en public » selon Ashley Tian, ancienne journaliste sportive à Shanghai, mais avec le bouche à oreille, la société chinoise est rapidement informée des accusations portées par Peng Shuai¹³¹⁴.

Peng Shuai elle-même ne s'exprime plus : depuis son message du 2 novembre, elle n'a plus d'activité sur les réseaux sociaux, ne fait plus d'apparition publique, ne répond plus aux prises de contact par la WTA (Women's Tennis Association, principal organisateur des tournois de tennis féminins dans le monde, dont Peng Shuai est membre)¹³¹⁵. Le 3 puis le 17 novembre 2021, interrogé sur la localisation de Peng Shuai lors d'une conférence de presse, le porte-parole du ministère des Affaires étrangères répond ne pas être au courant de l'accusation et que, la question posée n'étant pas une question diplomatique, elle ne relève pas de la compétence du ministère des

¹³⁰⁹ ZENG Jing, « #MeToo as connective action: A study of the anti-sexual violence and anti-sexual harassment campaign on Chinese social media in 2018 », *Journalism Practice*, vol. 14, 2020, p. 184

¹³¹⁰ BOYD Alexander et YU Alex, « Inside peng shuai's accusation against former top leader: #metoo, censorship, and resistance discourse », *China Digital Times*, 4 nov. 2021

¹³¹¹ *Ibid.* et DEFRANOUX Laurence, « #MeToo en Chine : une star du tennis accuse de viol un ancien vice-Premier ministre », *Libération*, 3 nov. 2021

¹³¹² GAN Nectar et XIONG Yong, « Chinese tennis star accuses former top Communist Party leader of sexual assault, triggering blanket censorship », *CNN*, 17 nov. 2021

¹³¹³ CHANG CHIEN Amy et STEVENSON Alexandra, « 'Where is **?': Fans in China Elude Censors to Talk About Peng Shuai », *The New York Times*, 2 déc. 2021

¹³¹⁴ *Ibid.*

¹³¹⁵ SMITH Jennifer, « Where is Peng Shuai? Serena Williams and World Tennis Association demand answers from China over missing star's safety as state media releases 'fake' proof of life email two weeks after she accused politician of rape », *Daily Mail*, 19 nov. 2021

Affaires étrangères¹³¹⁶. Le 14 novembre 2021, le directeur de la WTA, Steve Simon, demande aux autorités chinoises d'enquêter sur les allégations de Peng et de cesser la censure. Le 17 novembre 2021, le média d'État chinois anglophone, China Global Television Network, rapporte sur Twitter un courriel que Peng Shuai aurait adressé à Steve Simon : « *Les informations contenues dans le communiqué de presse de la WTA, y compris l'allégation d'agression sexuelle, ne sont pas vraies. Je n'ai pas disparu et je ne suis pas en danger. Je me suis juste reposée à la maison et tout va bien. Merci encore de vous soucier de moi* »¹³¹⁷. De nombreux indices rendent toutefois sceptiques sur la sincérité de ce courriel¹³¹⁸. Simon n'est pas convaincu, et le parti-État doit aussi s'assurer de convaincre la population chinoise que Peng est en sécurité. Le 18 novembre, Simon menace de suspendre les tournois organisés en Chine si aucune enquête n'est ouverte sur les accusations de Peng¹³¹⁹.

Le 19 novembre, Peng fait sa première réapparition sur les réseaux sociaux en publiant quatre photos d'elle-même sur WeChat, souriante, entourée de peluches et, semble-t-il, dans son appartement. Le lendemain, le média d'État Global Times publie trois vidéos présentées comme récentes, dans lesquelles Peng ne s'exprime pas – l'une où elle est annoncée parmi cinq autres invités dans un stade dont les tribunes sont quasiment vides, les deux autres où elle est attablée au restaurant avec son coach et une amie¹³²⁰. Simon ne voit dans ces vidéos aucune preuve de la liberté de l'athlète. Le 21 novembre, dans un communiqué très sommaire, le Comité international olympique déclare que Peng a discuté par appel vidéo avec Thomas Bach, Emma Terho et Lil Lingwei, et leur aurait affirmé être « *en sécurité et en bonne santé* »¹³²¹. Pour Simon, cet échange sur lequel le CIO se montre très secret n'est toujours pas une preuve de la liberté de Peng, et il exige que Peng soit autorisée à quitter le pays ou qu'elle soit autorisée

¹³¹⁶ « 彭帅长文指控中国前高官后遭网络审查 » (« Peng Shuai fait l'objet d'une cybercensure après une longue accusation portée contre un ancien haut fonctionnaire chinois »), *Radio France Internationale*, 3 nov. 2021 ; « 中国官媒发布“彭帅电邮” WTA 主席质疑真实性 » (« Les médias officiels chinois ont publié le "courriel de Peng Shuai", dont le président de la WTA a mis en doute l'authenticité »), *Deutsche Welle*, 25 nov. 2021

¹³¹⁷ DAVIDSON Helen, « The disappearance of Peng Shuai: what happened to the Chinese tennis star? », *The Guardian*, 19 nov. 2021

¹³¹⁸ *Ibid.* : le vocabulaire et la structure des phrases « *étaient similaires aux aveux forcés précédents des détenus en Chine, la capture d'écran comportait un curseur visible dans le texte, et la lettre n'a été publiée nulle part en Chine ou en chinois* ». De même, le 15 novembre 2021 (soit quatre jours avant la réapparition publique de Peng Shuai), le chercheur de l'Institut français des relations internationales (Ifri) Marc Julienne, spécialiste de la politique chinoise, prédisait : « *pour l'instant, elle a juste disparu de la scène médiatique, elle devrait réémerger. Il y a des chances qu'elle soit chez elle le temps que la polémique ne désenfle. Il va être difficile de porter une condamnation contre elle car c'est elle la victime. Le parti communiste l'a mise de côté et a censuré toute cette affaire sur tous les réseaux et l'internet chinois pour éviter toute instabilité. Peut-être que Peng Shuai va ressurgir et faire des excuses publiquement. Elle va répéter une ligne officielle qu'on lui aura donnée. A voir si elle pourra continuer sa carrière dans le tennis. Mais le parti communiste chinois devrait la laisser tranquille ensuite* » (GRIFFON Sarah, « Disparition de Peng Shuai : un phénomène "assez courant" selon un spécialiste de la Chine », BFM TV et RMC Sport)

¹³¹⁹ BURNETT Erin, MOGUL Rhea, REGAN Helen et GAN Nectar, « Peng Shuai: UN calls for proof of Chinese tennis star's whereabouts; WTA chairman willing to pull out of China », *CNN*, 20 nov. 2021

¹³²⁰ « Disparition de Peng Shuai : des photos et trois vidéos de la joueuse font leur apparition sur internet », *France Info*, 20 nov. 2021

¹³²¹ « L'affaire Peng Shuai place le CIO face à ses limites », *Le Figaro*, 23 nov. 2021

à parler en direct par téléconférence avec lui sans la présence d'autrui¹³²². Les exigences de Simon sont refusées et, le 1^{er} décembre, la WTA annonce retirer du calendrier féminin tous les tournois disputés en Chine¹³²³. Le boycott durera jusqu'au 18 septembre 2023, après que Steve Simon eut considéré Peng en sécurité¹³²⁴.

De notre étude du mouvement MeToo en Chine, on en tire plusieurs conclusions sur la feinte. Premièrement, malgré la censure systématique, méticuleuse et massive de ce mouvement depuis 2018, de nombreux messages MeToo ont continué à gagner une grande échelle de diffusion parce que des millions d'internautes chinois ont feinté les restrictions. On est donc en présence d'un jeu classique du chat et de la souris, où **les souris peuvent toujours feinter les restrictions imposées par le chat**, aussi coordonnées et généralisées soient ces restrictions.

En ce sens, le mouvement féministe chinois en ligne ne s'est pas éteint après les révélations de Peng Shuai. Le 28 janvier 2022, un utilisateur de Douyin publie une vidéo qui montre une femme perturbée mentalement, enchaînée à un mur par son époux dans un hangar délabré, à côté de la maison familiale où vivaient l'époux avec leurs huit enfants dans la ville de Xuzhou (dans le comté de Feng, lui-même membre de la province du Jiangsu). La vidéo suscite 1,92 milliards de clics sur différents réseaux sociaux chinois¹³²⁵. Face aux versions peu crédibles et contradictoires données par les autorités locales, de nombreux internautes chinois mènent leurs propres enquêtes sur l'histoire de la femme enchaînée et recueillent des témoignages sur la traite des femmes en Chine (notamment dans les provinces rurales du Jiangsu et de l'Anhui)¹³²⁶. Le blocage

¹³²² DE LA FUENTE Homero, « Chinese tennis star Peng Shuai tells International Olympic Committee she is 'safe and well' in video call », *CNN*, 22 nov. 2021

¹³²³ « Disparition de Peng Shuai : le président de la WTA, Steve Simon, annonce la suspension des tournois de tennis féminin en Chine », *France Info*, 1^{er} déc. 2021

¹³²⁴ « Steve Simon, patron de la WTA : "Peng Shuai est en sécurité et nous savons où elle se trouve" », *L'Équipe*, 24 mai 2023. Dans les faits, plusieurs facteurs expliquent probablement le revirement de Simon, notamment ceux rappelés par l'ancien joueur de tennis Arnaud Di Pasquale : la dépendance de la WTA à la Chine (« la WTA a investi massivement en Chine il y a quelques années (...) ; c'est grâce à la Chine qu'il y a eu beaucoup de beaux tournois qui ont été organisés, ce qui a permis à la WTA de vivre très grassement ; (...) ça crée forcément des déséquilibres économiques, et ils [la WTA] y reviennent [sur leur décision] ») ; et le fait que l'argument des droits de l'homme est difficilement tenable à long terme pour justifier le boycott de la Chine si la WTA ne boycotte pas les autres pays violant les droits fondamentaux (« DIP Impact – Affaire Peng Shuai : "la WTA est dépendante de la Chine, sa position n'était pas tenable" », *Eurosport*, 20 sept. 2023). Au surplus, les joueuses de la WTA se trouvaient pénalisées par ce boycott, notamment en raison de la perte des recettes apportées par les tournois en Chine comme l'explique Steve Simon : « après seize mois de suspension des compétitions de tennis en Chine et d'efforts continus pour atteindre notre objectif, aucun signe de changement n'est apparu. Nous en avons conclu que nous ne parviendrions jamais complètement à nos objectifs et qu'au bout du compte, ce sont nos joueuses et nos tournois qui paieront le prix fort pour leur sacrifice » (« Affaire Peng Shuai : les tournois de tennis féminins vont retourner en Chine, annonce la WTA », *The HuffPost*, 13 avr. 2023).

¹³²⁵ CAO Aowen et FENG Emily, « The mystery of the chained woman in China », *NPR*, 17 fév. 2022

¹³²⁶ *Ibid.* Les autorités locales de Xuzhou ont d'abord nié l'existence d'une traite d'êtres humains dans le cas de la femme enchaînée par son époux, au motif que leur mariage était légal (1^{ère} déclaration du 28 janvier 2022), puis ont soutenu que la femme enfermée était une jeune mendicante schizophrène recueillie et adoptée par un homme, avant d'être mariée à son fils, et qu'elle était enchaînée pour « l'empêcher de blesser autrui » (2^e déclaration du 30 janvier 2022). Elles sont ensuite revenues sur l'identité de la femme enchaînée – Xiao Hua Mei, et non Moxia Yang identifiée dans la première déclaration –, puis ont affirmé que le profil correspondait à celui d'une femme portée disparue du

des comptes des enquêteurs amateurs n'a pas empêché ces derniers de créer d'autres comptes sur les réseaux sociaux (feinte) pour continuer à partager des informations sur le sujet ; le silence des médias d'État sur le sujet et la suppression de nombreux témoignages par les réseaux sociaux n'ont pas empêché ce scandale d'être le sujet le plus tendance sur les réseaux sociaux chinois toute la semaine du 7 février 2022, devant les Jeux olympiques d'hiver de Pékin et la victoire de la skieuse acrobatique Eileen Gu ; les arrestations des utilisateurs-enquêteurs les plus actifs n'ont pas empêché les internautes chinois d'être sensibilisés sur le sujet, de publier des millions de messages de soutien à la femme enchaînée, de réclamer des mesures de lutte contre la traite des êtres humains et de protection des personnes atteintes de troubles mentaux¹³²⁷.

Confrontées à la pression de l'opinion publique sur internet, et aux enquêtes qui révèlent de plus en plus de cas de traites des femmes dans la Chine rurale, les autorités provinciales du Jiangsu ordonnent le 17 février 2022 une nouvelle enquête sur la femme enchaînée. Dans le cadre de cette enquête, six fonctionnaires sont arrêtés par la police et huit sont limogés pour avoir publié des fausses informations. À l'issue de l'enquête sont divulguée la véritable identité de la femme enfermée et publiée une chronologie détaillée des événements¹³²⁸. Une étude de 2022 confirme le rôle central joué par les utilisateurs féministes dans la diffusion de ce scandale sur Weibo et des messages dénonçant la traite des femmes dans les ruralités chinoises¹³²⁹. Grâce à la feinte, les féministes persistent donc à produire des R-DATA censurées par la puissance publique, et à leur faire acquérir une échelle de diffusion considérable.

Deuxièmement, **l'utilisation de la feinte à grande échelle a eu d'importantes répercussions sur la société chinoise**. Ainsi, après la première vague #MeToo de février 2018 rapportant de nombreuses violences sexuelles dans le cadre universitaire, l'Université de Pékin a institué une politique de tolérance zéro à l'égard du harcèlement sexuel (en avril 2018), et le ministère chinois de l'Éducation a institué des « *règles de moralité* » (en décembre 2019) pour les enseignants de l'enseignement supérieur qui leur interdisent d'enseigner à nouveau s'ils sont

village de Yagu au sud-ouest du Yunnan, après que sa mère l'ait confiée à une villageoise du nom de Sang pour un traitement médical ; selon Sang, Mei s'est égarée après être descendue du train (3^e déclaration du 7 février 2022). De nombreux internautes trouvent absurde cette version selon laquelle une mère confierait sa fille à une inconnue pour un traitement médical à 3000km du foyer familial. Enfin, les autorités locales ont fini par reconnaître que cette affaire relève de la traite des êtres humains (4^e déclaration du 10 février 2022), à la suite de quoi Sang, son mari et l'époux de Mei sont arrêtés.

¹³²⁷ *Ibid.* ; et KUO L. et LI L., « Saga of the chained mother of eight continues to roil China, inspiring rare social activism », *The Washington Post*, 25 fév. 2022 ; YUN Wang, « Les fonctionnaires réduisent au silence les demandes d'enquête émanant de civils. Les gens descendront-ils dans la rue par solidarité avec la mère des huit enfants ? » (官媒噤声民间推动调查 人们会上街声援八孩母亲 ?), *Radio Free Asia*, 16 fév. 2022. On précisera que, parmi les utilisateurs-enquêteurs, l'utilisatrice Wu Yi a été jugée dans un cadre secret pour avoir « *cherché à provoquer des conflits et troublé l'ordre public* », sans que l'on connaisse la peine prononcée et sans que l'on puisse retrouver Wu Yi après sa condamnation : « La situation des droits humains dans le monde. Rapport 2022-2023 », *Amnesty International*, 2023

¹³²⁸ WU Huizhong, « China's investigation confirms chained woman was trafficked », *AP News*, 23 fév. 2022

¹³²⁹ YAN Jiayi, « Hashtag activism, feminist counterpublics, and the myth of intersectionality: a case study of the emerging online discourse on Weibo #Feng County sex-trafficking case », Université de Liverpool, *Academia.edu*, 2022

reconnus coupables de harcèlement sexuel¹³³⁰. En août 2018, est annoncé un projet de loi contre le harcèlement sexuel en milieu professionnel – notons toutefois que, si le mouvement #MeToo a probablement accéléré l’annonce de ce projet de loi, il n’en a pas fait naître l’initiative¹³³¹. De même, en 2021, une fois le message de Peng Shuai supprimé, l’échelle de diffusion de la R-DATA « messages évoquant l’accusation contre Zhang Gaoli » a continué d’être amplifiée grâce à la feinte, ce qui a permis à l’accusation d’être connue par la population chinoise et par la société internationale malgré la censure très réactive (moins de 30 minutes après la publication du témoignage). Par conséquent, la connaissance par la population chinoise des violences sexuelles commises par Zhang Gaoli contre Peng Shuai, la suspension des tournois mondiaux de tennis féminin sur le sol chinois, et les pressions diplomatiques occidentales sont toutes des répercussions qui découlent du recours très répandu à la feinte par les utilisateurs chinois. Enfin, le recours à la feinte par les internautes chinois dans l’affaire de la femme enchaînée a permis d’amplifier l’échelle de diffusion des messages informant sur la traite des femmes en Chine, de sensibiliser la population à ce sujet, et a débouché sur une enquête sérieuse, l’arrestation et le licenciement de plusieurs fonctionnaires. L’emploi de la feinte par le mouvement féministe a donc effectivement eu d’importantes répercussions juridiques, institutionnelles, diplomatiques, sportives et sociales en Chine depuis 2018.

En somme, la feinte nous semble un bon exemple de la manière dont internet a permis à la population chinoise : de s’exprimer et de s’informer plus librement malgré une censure très réactive et coordonnée ; de voir ses messages acquérir une échelle de diffusion de plus en plus ample ; et de provoquer des changements sociaux, juridiques et institutionnels en Chine. La Chine est encore loin d’être un État qui contrôle efficacement l’échelle de diffusion des R-DATA produites dans son cyberspace. Surtout, la configuration de la feinte – comme celle de la migration étudiée précédemment – illustre combien **l’effet des techniques de restriction**

¹³³⁰ STUBBS-RICHARDSON Megan, GILBREATH Shelby, PAUL MacKenzie et REID Audrey, « It’s a global #MeToo: a cross-national comparison of social change associated with the movement », *Feminist Media Studies*, 4 juil. 2023. Se sont par ailleurs ajoutées des mesures locales à Pékin : le district de Dongcheng a exigé aux établissements scolaires de « signaler tous cas de harcèlement aux autorités éducatives dans les 10 minutes qui suivent l’incident et de présenter un rapport écrit dans les deux heures » ; « le district de Haidian a demandé aux écoles d’intégrer des mesures anti-harcèlement et d’inculquer aux élèves les dangers du harcèlement, les former à la prévention et les informer des répercussions juridiques que peuvent avoir de tels actes » ; le district de Fengai a fixé des critères pour évaluer la responsabilité du personnel éducatif, des chefs d’établissements et des professeurs en matière de harcèlement (« De nouvelles mesures contre le harcèlement scolaire à Beijing », *Le Quotidien du Peuple* [média d’État], 9 juil. 2018).

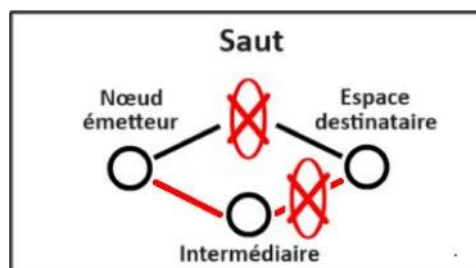
¹³³¹ Dès 2017, soit avant la diffusion du mouvement #MeToo, la déléguée Sun Xiaomei, membre de l’Assemblée Populaire Nationale, « a soumis au Comité permanent de l’[Assemblée] un projet de loi sur la discrimination d’emploi, en appelant à la construction d’une loi comportant des précisions sur les critères des discriminations et les mesures concrètes contre elles » (MALLET-JIANG Shuaijun, « La protection juridique des femmes au travail en Chine », *Mémoire(s), identité(s), marginalité(s) dans le monde occidental contemporain*, n° 28, 10 nov. 2022). Le harcèlement sexuel sur le lieu de travail est condamné par la loi chinoise depuis un amendement de 2005 qui modifie la Loi de 1992 pour la protection des droits et intérêts des femmes (《中华人民共和国妇女权益保障法》) mais l’infraction n’est pas définie par la loi, faisant de l’interdiction du harcèlement sexuel une ligne directrice davantage qu’une loi applicable. Le projet de loi annoncé en 2018 est adopté en 2020, et intégré au nouveau Code civil chinois (article 1010 du Chapitre 2). Le Code civil définit le harcèlement sexuel et oblige les employeurs à mettre en œuvre des mesures pour prévenir et enregistrer les plaintes, enquêter les traiter les affaires de harcèlement sexuel sur le lieu de travail.

sur une échelle de diffusion peut être limité voire neutralisé par le contournement. Enfin, comme la migration, la feinte peut être recourue par n'importe quel prescripteur pour contourner la restriction d'une R-DATA. Typiquement, le programmeur qui conçoit un logiciel malveillant peut contourner les restrictions posées par les logiciels antivirus en trouvant une formule de production qui n'est pas restreinte par l'antivirus. Ce faisant, il feint les restrictions de l'antivirus pour rendre possible le téléchargement de son logiciel malveillant sur une machine équipée de cet antivirus. Les restrictions posées par l'antivirus seront dans ce cas inefficaces pour réduire l'échelle de diffusion du logiciel malveillant.

B) Les configurations de contournement qui reposent sur des intermédiaires

1. Le saut

On appelle « saut » la situation dans laquelle un prescripteur numérique utilise un logiciel intermédiaire et/ou une machine intermédiaire pour accéder à une donnée. Le saut est recouru *de facto* par toute personne qui utilise internet, car les requêtes de cette personne sont nécessairement transmises par des machines intermédiaires (passerelles et routeurs IP) pour produire des données en ligne. Par exemple, si



un terminal transmet des données à la passerelle, qui les transmet elle-même à un routeur IP, qui les transmet directement au serveur destinataire, les données subissent trois sauts (terminal → passerelle, puis passerelle → routeur IP, puis routeur IP → serveur, v. ci-contre). Ici, le saut s'appuie sur un intermédiaire physique (machine), mais il peut aussi s'appuyer sur un intermédiaire logique (logiciel, tel un pare-feu).

Le saut peut aussi être recouru afin de contourner la restriction d'une R-DATA. C'est l'hypothèse qui nous intéresse ici. Dans ce cas, le saut correspond à la configuration dans laquelle le prescripteur numérique persiste à produire ou stocker une R-DATA sur le même espace logique avant et après la restriction, mais en utilisant un intermédiaire pour échapper à la restriction. À cette fin, de nombreux logiciels peuvent servir d'intermédiaire. On a déjà vu l'exemple des VPN, qui ont permis à des millions d'internautes russes de contourner les restrictions sur TikTok, ou les restrictions frappant Instagram. Dans ces deux cas, les utilisateurs se servent d'un logiciel intermédiaire (un VPN) pour accéder aux mêmes espaces logiques que ceux auxquels ils accédaient avant leur restriction (TikTok et Instagram). On a vu aussi que les internautes et gestionnaires d'applications peuvent utiliser des ports non brimés pour contourner la restriction d'un ou plusieurs ports.

Le saut est également la configuration qui correspond à l'usurpation d'adresses IP – méthode consistant à utiliser l'adresse IP d'autrui pour produire une requête d'accès. Dans ce cas, l'adresse IP est l'intermédiaire logique emprunté pour accéder à un espace logique (p. ex. pour utiliser l'abonnement Netflix d'autrui, pour utiliser la machine d'autrui située sur un territoire étranger afin de contourner le blocage d'un site web sur le territoire de l'usurpateur, pour mener des attaques par déni de service...). De même, des noms de domaine tiers peuvent être utilisés comme intermédiaires pour sauter une restriction de l'accès. Ce fut typiquement le cas de Telegram en Russie. En l'espèce, les lois Yarovaya promulguées en 2016 obligent les opérateurs de télécommunication russes à conserver durant six mois le contenu des appels vocaux, des images et des messages texte, et à conserver durant trois ans leurs métadonnées (coordonnées géographiques d'une photo, heure et date,

destinataire, expéditeur d'un message...). L'année suivante, un tribunal moscovite interprète les lois de 2016 comme obligeant Telegram à stocker sur ses serveurs les clés de chiffrement de toute correspondance des utilisateurs ¹³³². Telegram y oppose que les communications sur sa messagerie sont chiffrées de bout-en-bout, de sorte que les clés de chiffrement sont stockées sur les terminaux des utilisateurs. Les lois de 2016 obligeraient donc Telegram à abandonner le chiffrement de bout-en-bout. Pavel Durov, co-fondateur de Telegram, persiste à refuser d'adapter son application Telegram pour se conformer aux lois Yarovaya. Le 13 avril 2018, à la demande du Roskomnadzor, le tribunal du district Tagansky de Moscou ordonne aux opérateurs russes de bloquer l'accès aux noms de domaine de Telegram, et l'appel de Telegram devant la Cour suprême russe est rejeté¹³³³.

En réponse à cette décision de justice, l'entreprise Telegram Messenger Inc. recourt à une technique appelée « domain fronting »¹³³⁴. Cette méthode consiste à exploiter le protocole HTTPS pour utiliser des noms de domaines tiers (qui serviront à initialiser la connexion), et pour dissimuler le nom de domaine du destinataire définitif. En effet, une requête HTTPS indique à trois reprises le nom de domaine destinataire dans son datagramme : la requête DNS ; le Serveur Name Indication (SNI) du serveur destinataire ; et le nom de domaine du serveur destinataire qui emprunte le protocole HTTPS.

Requête HTTPS		
Requête DNS	SNI	HTTPS Host

Ces trois informations sont relatives à des protocoles différents – respectivement les protocoles DNS, TLS (protocole de sécurisation des échanges) et HTTPS (protocole de chiffrement des requêtes web). Seul le destinataire mentionné en HTTPS Host est chiffré jusqu'à son déchiffrement par le serveur HTTPS, donc ce destinataire est méconnaissable par les opérateurs. En principe, les trois destinataires désignent la même destination. Le domain fronting a pour objet de modifier les destinataires indiqués dans les champs « Requête DNS » et « SNI », en y désignant des noms de domaine (p. ex. imaginarynetwork.org) hébergés par le même fournisseur d'hébergement (p. ex. Amazon Web Service) que le nom de domaine restreint (p. ex. telegram.org). De cette manière, l'opérateur de transmission de données voit seulement les domaines destinataires mentionnés dans les champs DNS et SNI (imaginarynetwork.org), mais ne voit pas le domaine caché dans le champ HTTPS (telegram.org).

L'application qui recourt au domain fronting (Telegram) utilise alors des domaines tiers comme intermédiaires pour faire rebondir le trafic vers cette application : l'opérateur transmet la requête vers le serveur DNS hébergeant le nom de domaine imaginarynetwork.org, puis les serveurs DNS d'imaginarynetwork.org redirigent la requête vers telegram.org. Dès lors, l'opérateur ne peut plus différencier le trafic destiné au domaine restreint (telegram.org) par rapport au trafic destiné aux domaines hébergés par le même fournisseur d'hébergement et

¹³³² Tribunal du district de Meschansky (Moscou), aff. n° 5-1794/2017 du 16 oct. 2017

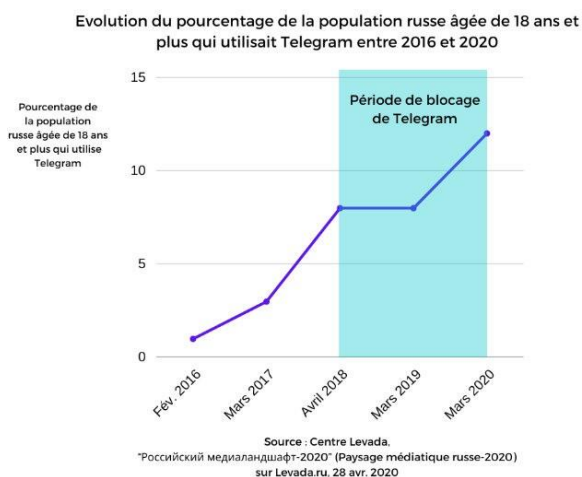
¹³³³ « A Moscow court sanctions the Russian government's request to block Telegram », *Meduza*, 13 avr. 2018

¹³³⁴ BURGESS Matt, « This is why Russia's attempts to block Telegram have failed », *Wired*, 28 avr. 2018

mentionnés dans la requête HTTPS domain-fronted (imaginarynetwork.org). Cette technique a pour intérêt de n'exiger aucun effort de contournement de la part des utilisateurs russes de Telegram : la requête HTTPS domain-fronted est automatiquement générée par le client (*i.e.* l'application mobile Telegram). Les utilisateurs russes n'ont donc qu'à utiliser classiquement l'application Telegram disponible sur leur smartphone pour contourner la censure par les opérateurs.

En avril 2018, dans le contexte durecours au domain fronting par Telegram, Google et le service CloudFront d'Amazon désactivent la possibilité d'utiliser leur réseau à des fins de domain fronting, empêchant ainsi Telegram de se servir des noms de domaines hébergés par ces deux fournisseurs d'hébergement pour contourner la censure russe¹³³⁵. Les restrictions par les opérateurs russes et par les hébergeurs Google et Amazon CloudFront n'ont pas empêché Telegram de poursuivre son domain fronting en exploitant les noms de domaine hébergés par d'autres fournisseurs

d'hébergement (notamment des fournisseurs de CDN, comme Akamai, CloudFlare...). Ainsi, malgré la censure très active (le Roskomnadzor a fait bloquer plus de 600 000 adresses IP redirigeant vers Telegram¹³³⁶), Telegram gagne de nouveaux utilisateurs russes au lieu d'en perdre (graphique ci-contre).



Le 19 juin 2020, le Roskomnadzor raye Telegram de la liste des sites bloqués, considérant que Telegram avait « *accepté de contribuer aux enquêtes sur l'extrémisme* »¹³³⁷. Ni le Roskomnadzor, ni Telegram n'ont commenté les changements apportés par la messagerie instantanée pour parvenir à cet accord. On trouve cependant une partie de la réponse dans la FAQ de Telegram. À la question « Comment chiffrez-vous vos données », Telegram y répond que les échanges privés et de groupe font l'objet d'un « *chiffrement serveur-client* », *i.e.* d'un chiffrement unilatéral par lequel seul le serveur de Telegram hébergé la clé de chiffrement des messages¹³³⁸. L'entreprise peut donc à tout moment déchiffrer ces messages : en principe, les communications sur Telegram ne sont plus chiffrées de bout-en-bout. Par exception, poursuit la FAQ, les échanges secrets font toujours l'objet d'un « *chiffrement client-client* », *i.e.* d'un chiffrement de bout-en-bout. Le principe est ainsi devenu l'exception : par défaut, les correspondances des utilisateurs de Telegram ne sont plus chiffrées de bout-en-bout, alors que c'est précisément à cause du chiffrement de bout-en-bout que Telegram avait été bloqué en Russie en 2018. Les clés de chiffrement de tous les utilisateurs de Telegram dans le monde sont désormais stockées sur les serveurs de Telegram, comme l'exigeait le Roskomnadzor. C'est

¹³³⁵ BRANDOM Russell, « A Google update just created a big problem for anti-censorship tools », *The Verge*, 18 avr. 2018 ; MACCARTAGH Colm, « Enhanced Domain Protections for Amazon CloudFront Requests », sur [Aws.amazon.com](https://aws.amazon.com), 27 avr. 2018

¹³³⁶ Comme on l'a déjà rapporté, le doctorant Lincoln Pigman a constaté que le volume d'adresses IP inscrites sur liste noire en Russie est passé de 650 000 à 30 000 le jour où Telegram a été débloqué : PIGMAN L., « In memoriam: Russia's ban on Telegram, 2018-2020 », *Riddle Russia*, 22 juin 2020

¹³³⁷ « Russia lifts ban on Telegram messaging app after failing to block it », *Reuters*, 18 juin 2020

¹³³⁸ « FAQ », sur [Telegram.org](https://telegram.org) [consultée le 14 avril 2023] ; v. aussi KRAUS Rachel, « What Russians should keep in mind when using Telegram », *Mashable*, 4 mars 2022

une demi-victoire pour la Fédération russe, car les utilisateurs qui le souhaitent peuvent toujours chiffrer leurs correspondances de bout-en-bout en utilisant la fonctionnalité « échanges secrets ». Cette fonctionnalité n'est utilisable que pour des échanges inter-individuels – donc tous les échanges de groupe sont aisément déchiffrables –, mais les terroristes, pédophiles et marchands de produits illicites peuvent toujours communiquer par échanges secrets sur Telegram afin de rendre leurs messages quasi-indéchiffrables.

Surtout, le point qui nous intéresse ici réside dans l'**inefficacité des techniques de blocage employées pour réduire l'échelle de diffusion de Telegram en Russie, à cause d'un fort recours au saut** par le gestionnaire de l'application et les utilisateurs russes qui se sont appuyés sur des noms de domaine tiers pour rebondir vers Telegram. Cette inefficacité semble avoir créé un précédent en Russie, qui explique probablement l'incohérence de mars 2022 : après avoir qualifié l'entreprise Meta d'ennemie de la Nation, la Fédération a restreint l'accès à tous les produits de Meta sans imposer de restriction à WhatsApp. Il est possible que le précédent Telegram (contournement massif des restrictions contre un réseau social populaire) ait conduit le gouvernement à ne pas restreindre l'accès à WhatsApp, sachant que WhatsApp était déjà l'application la plus utilisée en Russie avant les restrictions de février-mars 2022¹³³⁹. En somme, le saut a permis de faire croître l'échelle de diffusion de Telegram en Russie malgré les restrictions mises en œuvre.

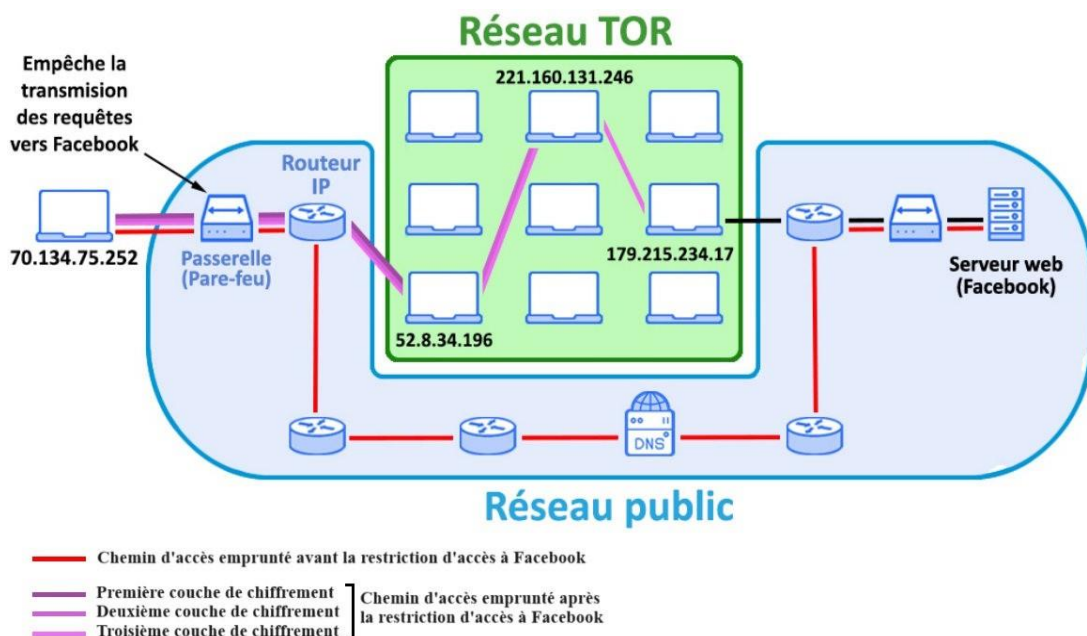
Outre les noms de domaine, les proxys sont d'autres intermédiaires utilisés pour le saut. Un proxy est un logiciel hébergé sur un serveur qui sert d'intermédiaire entre deux machines – pour améliorer la confidentialité des données, leur sécurité, les performances du processus d'accès (accélération de l'accès, répartition des charges...) etc. Le serveur proxy peut être utilisé de deux façons : il peut être utilisé en frontal du client, auquel cas le terminal qui stocke le client du proxy (*i.e.* le logiciel local correspondant au proxy) communique directement avec le serveur proxy ; et il peut être utilisé en frontal d'un serveur web (par ex. le serveur de Facebook), auquel cas le serveur web communique directement avec le serveur proxy sans que le client de l'utilisateur ait connaissance dudit serveur. Utilisé en frontal d'un serveur web, le serveur proxy est appelé « proxy inverse ». Le proxy inverse est employé à des fins très diverses, comme le chiffrement SSL (pour sécuriser l'accès à un site web selon le protocole HTTPS), la surveillance des données transitant par le serveur web, le filtrage de données ordonné par le serveur web puis exécuté par le serveur proxy (tel le filtrage de logiciels malveillants par un serveur proxy hébergeant un logiciel antivirus), la mise en cache de données pour faciliter et accélérer l'accès de l'utilisateur au serveur web etc.

Les proxys peuvent aussi être employés à des fins de contournement. Par exemple, si un serveur web restreint son accès aux seules machines résidant sur son territoire (par exemple les États-Unis), l'utilisateur résidant à l'étranger peut emprunter un serveur proxy situé aux États-Unis pour accéder à ce serveur web. Inversement, si les opérateurs d'un pays restreignent l'accès à un serveur web étranger (par ex. TikTok), l'utilisateur résidant dans ce pays peut emprunter un serveur proxy situé à l'étranger dont l'accès n'est pas restreint pour que ce dernier redirige les requêtes de l'utilisateur vers le serveur web de TikTok. De même, un serveur proxy peut substituer l'adresse IP source (à l'origine des requêtes) par sa propre adresse IP, ce qui a pour

¹³³⁹ En mars 2022, 66% de la population russe âgée de 18 ans et plus utilisait WhatsApp (devant les 65% de VK) ; ils étaient 64% en mars 2021 (devant les 44% des VK), soit un an avant les restrictions : « Internet, Réseaux sociaux et VPN » (Интернет, социальные сети и VPN), sur *Levada.ru*, 8 avril 2022. Sur le sujet v. aussi MEAKER Morgan, « Why WhatsApp Survived Russia's Social Media Purge », *Wired*, 21 mars 2022

effet d'anonymiser les requêtes de l'utilisateur auprès du serveur web. Ou encore, un logiciel proxy installé sur le terminal de l'utilisateur (*i.e.* un client proxy) peut simuler l'activité d'un serveur proxy sur ce terminal, ce qui permet à des machines tierces d'utiliser ce terminal comme voie d'accès à un service¹³⁴⁰.

Enfin on étudie les darknets comme dernier outil de contournement par saut. Un darknet est un réseau qui exploite les infrastructures d'internet pour y superposer ses propres protocoles réseau (généralement anonymisants) par-dessus les protocoles réseau d'internet. Concrètement, l'utilisateur doit donc préalablement accéder à internet pour atteindre un darknet régi par d'autres règles de communication qu'internet. On étudie ici le darknet TOR. TOR s'appuie sur le protocole IP. Les utilisateurs bénévoles mettent leur adresse IP à disposition de tous les utilisateurs de TOR. Ces adresses IP mises à la disposition d'autrui sont appelés « nœuds TOR ». Toute requête qui traverse le réseau TOR emprunte trois nœuds TOR avant d'arriver à destination, *i.e.* effectue trois sauts au sein du darknet. Chaque fois que la requête change de nœud TOR, elle porte l'adresse IP du dernier nœud emprunté, de sorte que le destinataire définitif de la requête ne connaîtra que l'adresse IP du troisième nœud TOR emprunté. Les requêtes sont chiffrées jusqu'à parvenir au réseau TOR, et sont chiffrées à l'intérieur du réseau TOR, mais ne sont plus chiffrées lorsqu'elles quittent le darknet. Cette méthode de chiffrement est appelée « chiffrement en oignon » : la requête de l'utilisateur est enveloppée par trois couches de chiffrement qui, à l'image de l'oignon, sont retirées les unes après les autres au fil de ses sauts dans le réseau TOR. Les utilisateurs de TOR peuvent accéder aussi bien à des applications ou des terminaux situés en-dehors du réseau TOR (sur le réseau internet public) qu'à des applications et terminaux situés dans ce darknet (tels les noms de domaine en <.onion> qui ne sont pas régis par l'Icann). Un internaute peut ainsi se servir de TOR pour contourner les restrictions de l'accès à Facebook (ou à n'importe quelle autre application) par son opérateur.



¹³⁴⁰ Ce service était par exemple proposé par l'application uProxy lancée en 2013, devenue Outline VPN en 2018 : CUVELIER Frédéric, « uProxy : Google contourne la censure », *Clubic*, 22 oct. 2013

En somme, si un régulateur restreint l'accès à un service, les prescripteurs peuvent se servir de divers intermédiaires – VPN, ports, adresses IP, noms de domaine, proxys, darknets... – pour sauter la restriction. Les outils de contournement par saut ici pris en exemple ne couvrent évidemment pas toutes les techniques de contournement par saut. Surtout, plusieurs outils de contournement par saut peuvent être combinés. Par exemple, l'auteur d'une requête peut utiliser un VPN pour accéder à TOR, auquel cas il devient extrêmement difficile de remonter jusqu'à cet auteur. De même, l'application Orbot est un proxy qui fait le lien entre le terminal de l'utilisateur et le réseau TOR. Il permet ainsi à l'utilisateur d'un smartphone de traverser les nœuds TOR pour accéder à des navigateurs web ou à des moteurs de recherche, pour communiquer sur des messageries instantanées et sur des réseaux sociaux de partage de contenus, pour utiliser des plateformes de partage de vidéos etc. Ce faisant, Orbot donne à l'utilisateur la possibilité d'accéder, depuis TOR, à des applications censurées dans son pays – donc de produire des R-DATA. Ou encore, le navigateur web Brave Browser propose à ses utilisateurs un onglet « navigateur privé » qui les renvoie vers TOR à l'aide d'un proxy. De cette façon, les utilisateurs de Brave Browser peuvent directement utiliser TOR pour accéder à leurs applications habituelles en traversant TOR.

2. L'affranchissement



Enfin, on identifie une autre configuration de contournement proche du saut : l'affranchissement. On appelle « affranchissement » la configuration dans laquelle, une fois la restriction intervenue, le prescripteur recourt non seulement à un intermédiaire mais change par ailleurs l'espace logique auprès duquel il accède à une R-DATA. Il s'agit d'une combinaison du saut et de la migration : un intermédiaire est utilisé pour migrer vers un espace logique.

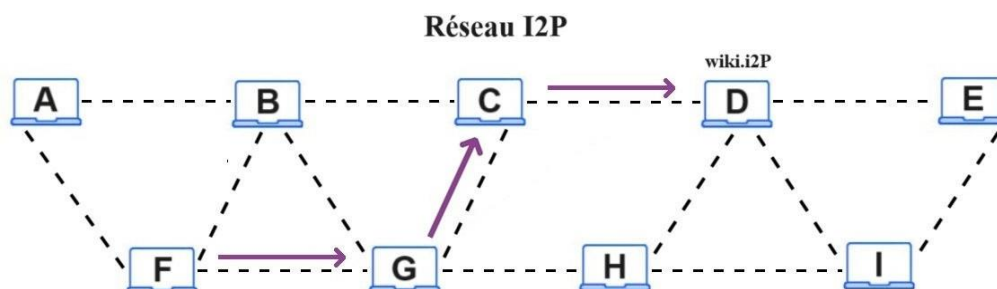
Prenons l'exemple d'un vendeur de contrefaçons sur Amazon qui voit son compte supprimé en raison de ses activités illicites. Pour contourner la restriction qui le frappe, il peut alors continuer à vendre ses contrefaçons sur un « marché darknet », *i.e.* sur un marché noir hébergé dans un darknet. Dans ce cas, le vendeur persiste à produire la R-DATA « vente de contrefaçons en ligne » en quittant Amazon pour un marché darknet (migration) au moyen d'un intermédiaire (TOR). Ce faisant, il s'affranchit entièrement de la restriction imposée par Amazon.

On a vu que TOR donne la possibilité d'accéder à des noms de domaine portant le TLD <.onion>, donc fournit des espaces logiques qui peuvent servir de destinataires définitifs (à savoir les noms de domaine <.onion>). C'est de cette manière que notre marchand de contrefaçons peut s'affranchir d'Amazon, en vendant par exemple ses marchandises sur le marché darknet portant le nom de domaine <oxsfyfyf3rmxwzvsozhze4awcwtbomwd2butx7fvdkl2nfks4tmno4qd.onion>¹³⁴¹. Les internautes peuvent aussi migrer vers d'autres darknets que TOR pour s'affranchir d'une restriction. On s'intéresse au cas I2P. Le darknet I2P (*Internet Invisible Project*)

¹³⁴¹ TOR ne possède pas d'équivalent au système DNS, donc les noms de domaine ne sont pas retranscrits dans un format intelligible. En octobre 2023, le domaine en <.onion> donné dans notre exemple correspondait au marché darknet Vice City Market, mais les adresses <.onion> peuvent régulièrement changer.

partage quelques traits communs avec TOR. Comme pour TOR, les requêtes effectuent plusieurs sauts dans le réseau I2P et se voient appliquées un chiffrement en oignon durant leur transmission (plusieurs couches de chiffrement sont levées au fil des sauts). Comme TOR, des applications peuvent être hébergées sur I2P (en HTTP ou HTTPS, avec le TLD <.i2p>).

Cependant des différences notables séparent ces deux darknets. Premièrement, I2P ne repose pas sur du bénévolat contrairement à TOR : toutes les machines connectées à I2P jouent le rôle de routeurs et de serveurs I2P. En d'autres termes, tout utilisateur d'I2P peut servir de routeur pour transmettre les requêtes dans le réseau I2P, mais peut aussi constituer un serveur pour héberger une application accessible sur I2P. Deuxièmement, les machines ne sont pas identifiées par leurs adresses IP au sein du réseau I2P, mais par une clé publique de chiffrement. Chaque machine connectée à I2P se voit attribuée une clé publique unique ; et les tables de routage, au lieu de répertorier les adresses IP des machines connectées au routeur, recense les clés publiques des machines connectées au routeur. Cela signifie que, sur I2P, les destinations sont des clés de chiffrement et non des adresses IP. Troisièmement, chaque routeur I2P participe à la transmission des requêtes par les autres routeurs, ce qui rend impossible d'identifier le volume de trafic qui provient d'une machine en particulier. Quatrièmement, chaque utilisateur choisit les nœuds I2P empruntés par sa requête pour parvenir à destination – donc chaque utilisateur crée son propre « tunnel de chiffrement ». Cinquièmement, I2P est un réseau autonome, c'est-à-dire qu'il n'est pas conçu pour permettre à l'utilisateur d'accéder au réseau internet public depuis le réseau I2P : contrairement à TOR, l'utilisateur d'I2P navigue uniquement au sein d'I2P (à moins d'utiliser un out-proxy faisant le lien entre I2P et internet)¹³⁴².

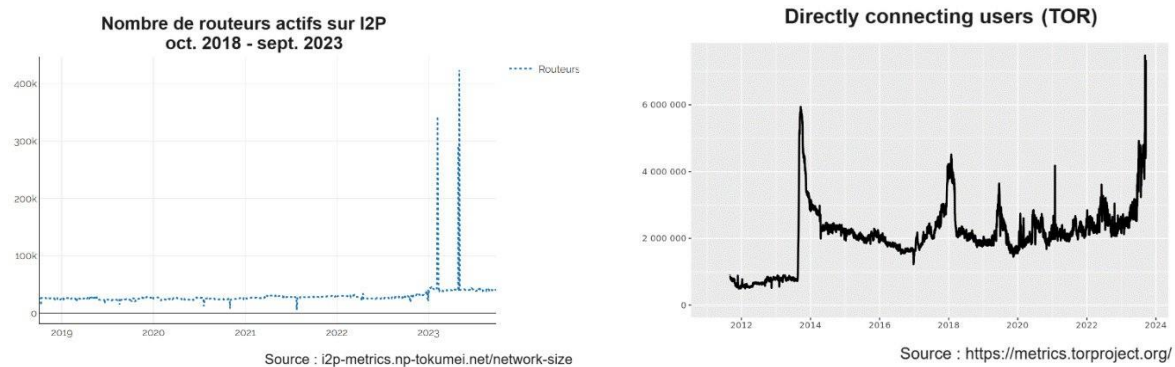


Concrètement, sur le schéma ci-haut, si la machine F souhaite atteindre le site web <wiki.i2p> hébergé par la machine D, la requête pourra traverser les nœuds G et C. Le routeur G sait que la requête lui est transmise par F, mais G ignore si F est le producteur originel de la requête ou s'il se contente de relayer une requête originellement produite par A ou B (nœuds connectés à F). Quant au routeur suivant, le nœud C, il ignore totalement l'implication de F dans ce processus ; il sait seulement que la requête lui est transmise par G, et qu'il doit la retransmettre à D¹³⁴³. Il est donc quasiment impossible de remonter jusqu'à F et de l'identifier comme l'auteur originel de la requête transmise sur I2P.

¹³⁴² Pour examiner en détail le fonctionnement d'I2P, v. PHONG HOANG Nguyen, KINTIS Panagiotis, ANTONAKAKIS Manos et POLYCHRONAKIS Michalis, « An Empirical Study of the I2P Anonymity Network and its Censorship Resistance », Internet Measurement Conference 2018, *ArXiv*, nov. 2018

¹³⁴³ On reprend ici l'exemple proposé dans la vidéo « I2P – Le réseau internet invisible et anonyme » publiée le 27 décembre 2015 par youtubeur Paf Le Geek, un créateur de contenus spécialisé dans les technologies de protection de la vie privée

Entre octobre 2018 et septembre 2023, le nombre d'utilisateurs actifs d'I2P est passé d'environ 20-25 000 à 35-40 000. Quant au nombre d'utilisateurs actifs de TOR, il est passé d'un peu moins d'un million en 2011 à 7,5 millions en septembre 2023¹³⁴⁴.



Les darknets peuvent être utilisés à des fins très diverses, notamment la protection de la vie privée. Mais ils sont aussi des espaces utiles pour diffuser largement des R-DATA fortement restreintes sur le réseau internet public. Une étude démontre ainsi que, en 2014, l'accès à des contenus pédopornographiques sur TOR représentait 83% de l'ensemble des requêtes émises sur le darknet (*i.e.* 83% du trafic total de TOR) tandis que 2% seulement des sites web hébergés sur TOR étaient des sites pornographiques¹³⁴⁵. En 2020, une autre étude estime qu'environ 6,7% des utilisateurs quotidiens de TOR l'utilisent à des fins de maltraitance d'enfants, de ventes et d'achats illicites de drogues, et de distribution de logiciels malveillants¹³⁴⁶. Précisément, ce pourcentage descendait à 4,8% dans les pays codifiés « non libres » du fait de leur régime politique (Chine, Russie, Algérie...), mais s'élevait au contraire à 7,8% dans les pays codifiés « libres » (États-Unis, Union européenne, Australie, Canada...). La majorité des utilisateurs de TOR semble s'en servir dans le but de préserver leur vie privée ou de contourner les censures gouvernementales.

En offrant aux prescripteurs numériques d'importantes capacités d'affranchissement, les darknets permettent à ces prescripteurs de persister à produire, dans des darknets, des R-DATA restreintes sur le réseau internet public. Du point de vue de la régulation, cela pose deux problèmes de taille. En premier lieu, les darknets entravent la réduction de l'échelle de diffusion de nombreuses R-DATA – comme la production et la consultation de contenus pédopornographiques, la vente illicite d'armes et de drogues *via* internet, le commerce illégal de logiciels malveillants et de données personnelles (passeports et cartes d'identité, cartes bancaires,

¹³⁴⁴ Le pic de connexions à TOR enregistré dans la deuxième moitié de 2013 coïncide avec la date des révélations d'Edward Snowden. En revanche, on ne sait pas expliquer ce qui a provoqué la forte recrudescence du nombre d'utilisateurs de TOR depuis la mi-2023.

¹³⁴⁵ OWEN Gareth et SAVAGE Nick, « The Tor Dark Net », *Centre for International Governance Innovation*, sept. 2015, p. 6. Les sites de crypto marché (marchés noirs sur les darknets) représentaient alors 3% du trafic, les sites dédiées à la vente de drogues 2%, les wikis 2%, les forums 2%, les annuaires répertoriant les sites en <.onion> 1%, et les autres catégories de sites se partageaient les 7% restants (sites d'hébergement, porno, jeux d'argent, armes, chat, actualités, livres, blog, hacking, recherches, anonymat, contrefaçons, lanceurs d'alertes, courriel, bitcoin et fraude).

¹³⁴⁶ JARDINE Eric, LINDNER Andrew et OWENSON Gareth, « The potential harms of the Tor anonymity network cluster disproportionately in free countries », *Proceedings of the National Academy of Sciences*, vol. 117, déc. 2020

mots de passe...), la vente de faux titres financiers (action, stock-option, obligations...), l'embauche de tueurs à gage etc. En second lieu, et en conséquence du premier point, les darknets facilitent l'essor d'une économie parallèle illicite – faussaires, marchands de drogues, d'armes, de logiciels malveillants, d'abus sexuel...

On reste sur l'exemple des marchés darknet. La première transaction initiée en ligne dans l'histoire du réseau numérique fut un trafic de drogue : vers 1971 ou 1972, des étudiants des universités de Stanford et du MIT se sont servis d'Arpanet pour organiser la vente de marijuana¹³⁴⁷. En 2010, Adam Bomb crée le premier marché reposant sur un darknet (TOR) : le Farmer's Market (lancé en 2006, mais déposé sur TOR en 2010). La plateforme est toutefois fermée par le FBI en 2012, grâce aux paiements par PayPal et Western Union qui ont permis de retracer les transactions¹³⁴⁸. En février 2011, Ross Ulbricht fonde Silk Road, premier marché darknet à utiliser la cryptomonnaie Bitcoin pour empêcher de retracer les paiements. Silk Road devient aussi le premier marché darknet qui bénéficie d'une large couverture médiatique et d'une grande base d'utilisateurs. Ulbricht est arrêté le 2 octobre 2013, et la fermeture de Silk Road entraîne l'essor d'une nuée de marchés darknet – Silk Road 2.0, Agora, Pandora, Evolution, Middle Earth, Nucleus, Black Bank, Alpha Bay, TheRealDeal, Babylone¹³⁴⁹... En novembre 2014, l'opération Onymous menée par le FBI et la National Crime Agency britannique permet de saisir 27 sites cachés (dont Silk Road 2.0) et 12 petits marchés darknet. S'ensuit une multitude d'opérations policières : en juillet 2015, la police italienne et Europol font fermer Babylone ; en avril 2017, dans le cadre d'une enquête internationale contre le trafic de drogue, la police italienne arrête trois vendeurs de drogue très actifs sur le marché darknet IDC (Italian Darknet Community) ; en juillet de la même année, l'opération Bayonet fait fermer les marchés AlphaBay et Hansa ; en août de la même année, le coadministrateur de Dream Market est arrêté, et la plateforme ferme en 2019 ; en 2021, l'administrateur de DarkMarket, alors le plus grand marché darknet, est arrêté dans le cadre d'une opération internationale coordonnée par Europol, et les 20 serveurs qui hébergeaient DarkMarket sont saisis ; en avril 2022, le marché Hydra est démantelé par la police allemande¹³⁵⁰.

Malgré les efforts policiers internationaux et les fermetures successives de marchés darknet, le nombre d'utilisateurs de ces marchés et le volume de transactions ne cessent de croître : en 2012, le Farmer's Market cumulait 3 000 utilisateurs, et a généré 2,5 millions de dollars de transactions ; en 2013, Silk Road comptait 118 000 utilisateurs (115 000 acheteurs et 3 000 vendeurs), pour un volume transactions de 213 millions de dollars (dont 183 millions en médicaments) ; en 2017, AlphaBay totalisait 240 000 (200 000 acheteurs et 40 000 vendeurs) à 400 000 utilisateurs, pour un volume de transactions supérieur à 1 milliard de dollars ; en 2021, DarkMarket comptait 500 000 utilisateurs avant sa fermeture ; en 2022, la saisie des serveurs d'Hydra révèle une base

¹³⁴⁷ MARKOFF John, *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*, préc., Penguin Books, 2006

¹³⁴⁸ « US busts online drugs ring Farmer's Market », *BBC*, 17 avr. 2012

¹³⁴⁹ « Silk Road successors », *The Economist*, 29 mai 2015

¹³⁵⁰ Sur ces événements, v. BEWLEY-TAYLOR David R. et TINASTI Khalid, *Research Handbook on International Drug Policy*, *Elgar*, 2020, p. 357s. ; CAMPBELL Ian Carlos, « Authorities have taken down the dark web's largest illegal marketplace », *The Verge*, 13 janv. 2021 ; TIDY Joe, « Hydra: How German police dismantled Russian darknet site », *BBC*, 6 avr. 2022

de 17 millions d'utilisateurs pour un volume de transactions de 2 milliards de dollars sur l'année 2021 et de plus de 5 milliards depuis 2017¹³⁵¹.

Comme pour les autres configurations de contournement étudiées, on constate donc que l'affranchissement peut limiter voire neutraliser totalement l'efficacité d'une technique de restriction. En l'espèce, la technique de la suppression de données sur internet (précisément la suppression, grâce à la saisie des serveurs, des fichiers hébergés sur internet constitutifs des plateformes de marchés darknet) n'a pas permis de réduire l'échelle de diffusion de la R-DATA « création et utilisation de marchés noirs en ligne ». Les exemples d'affranchissement ne se limitent évidemment pas aux marchés darknet. On a déjà rencontré l'exemple de Nord-coréens qui – avant le filtrage étatique de la Wifi via le réseau Mirae – se connectaient au Wifi des touristes, ambassades et ONG pour pouvoir se connecter au réseau internet public international. En agissant ainsi, ils se sont appuyés sur des intermédiaires (les machines des touristes, ambassades et ONG) pour quitter un espace logique (le cyberspace nord-coréen) au profit d'un autre (les cyberspaces étrangers, notamment chinois et sud-coréen). Ce faisant, ils se sont affranchis des restrictions nord-coréennes d'accès à internet.

C) Les configurations de contournement qui reposent sur des périphériques accessoires

Enfin, on identifie un dernier type de configuration de contournement, qui repose spécifiquement sur le recours à des périphériques accessoires (clé USB, disque dur, cartes mémoires, disques de stockage optique comme les CD ou DVD...). On retrouve ici les configurations de la feinte et de l'affranchissement, réalisables avec de tels périphériques. Les schémas déjà utilisés sont applicables pour modéliser ces configurations par périphériques ; il suffit d'ajouter un noeud « périphérique » en amont du noeud émetteur dans les schémas de la feinte et de l'affranchissement.

• La feinte par périphérique accessoire

On appelle « feinte par périphérique accessoire » la configuration de contournement dans laquelle un prescripteur numérique persiste à produire ou stocker une R-DATA sur le même espace logique malgré la restriction, en se servant d'un périphérique accessoire pour générer une formule de production non restreinte de cette R-DATA. Comme pour la feinte effectuée sans périphérique accessoire, la feinte par périphérique accessoire peut être pratiquée localement (si l'espace logique destinataire de la requête est présent sur la machine de production de la requête) ou en ligne (si l'espace logique destinataire de la requête est présent sur une autre machine que celle ayant produit requête).

On s'intéresse ici à des exemples de feinte locale par périphérique accessoire. Par exemple, un prescripteur numérique peut stocker sur un disque dur externe des contenus

¹³⁵¹ Pour le Farmer's Market : KIM Victoria, « Dutch national pleads guilty to running online marketplace for drugs », *Los Angeles Times*, 3 sept. 2014. Pour Silk Road : Bureau du procureur des États-Unis du district sud de New York, « Senior Adviser To The Operator Of The Silk Road Online Black Market Sentenced To 20 Years In Prison », *Justice.gov*, 11 juil. 2023. Pour AlphaBay : Office of Public Affairs, « AlphaBay, the Largest Online "Dark Market", Shut Down », *Justice.gov*, 20 juil. 2017 ; « Darknet Takedown. Authorities Shutter Online Criminal Market AlphaBay », *Fbi.gov*, 20 juil. 2017. Pour DarkMarket : Europol, « DarkMarket: world's largest illegal dark web marketplace taken down », 12 janv. 2021 ; CIMPANU Catalin, « AlphaBay Dark Web Market Taken Down After Law Enforcement Raids », *Bleeping Computer*, 14 juil. 2017. Pour Hydra : MANACH Jean-Marc, « La police saisit Hydra, la plus grosse des plate-formes du "dark web" », *NextInPact*, 7 avr. 2022

pédopornographiques ou représentant des violences sexuelles entre adultes, afin de contourner les restrictions et la surveillance frappant l'accès à de tels contenus. Un autre exemple classique est celui des CD-ROM et des DVD-ROM utilisés pour consommer illégalement des biens culturels. Dans ce cas, un prescripteur numérique peut acquérir légalement ou illégalement des biens culturels (films, musiques, séries TV, spectacle vivant, documentaire...), les stocker sur le CD ou le DVD, puis remettre le CD/DVD à d'autres prescripteurs numériques pour leur permettre de consommer illégalement ces biens¹³⁵².

De même, en Corée du Nord, la consommation illicite de films étrangers à l'aide de périphériques accessoires est très répandue. Durant les années 1990, la famine a provoqué l'essor de nombreux marchés noirs (physiques), sur lesquels étaient vendus de la nourriture et des biens en contrebande – dont des films étrangers. C'est le début d'une demande nord-coréenne croissante pour la consommation de films étrangers. Au début des années 2000, les films vendus sur le marché noir le sont d'abord sous la forme de DVD et, depuis les années 2010, le sont sous la forme de clés USB et de cartes mémoire¹³⁵³. Dans la première moitié des années 2010, apparaît le « notel », un petit lecteur multimédia qui permet de lire des DVD et d'y brancher une clé USB ; les contenus illicites sont stockés sur la clé USB et, en cas d'inspection policière inattendue, le DVD contient un film de propagande approuvé par l'État (« je regardais un film légal »). En 2015, on estimait que la moitié des ménages urbains nord-coréens possédait un notel : « *les gens échangent des feuillets, de la musique pop, des films hollywoodiens et des programmes d'information sud-coréens* »¹³⁵⁴. En 2022, une étude estime à 76% la probabilité qu'un nord-coréen de 19-29 ans partage avec un ami, et dans son propre domicile, des contenus sud-coréens non-fictifs via une clé USB ; cette probabilité s'élevait à 57% pour les nord-coréens de 30-49 ans qui partagent avec un ami, et dans le domicile de cet ami ou d'un tiers, des textes étrangers non-fictifs via une tablette ou un téléphone nord-coréen ; et la probabilité était de 43% pour qu'un nord-coréen de 19-29 ans partage avec un étranger et à l'extérieur du domicile des enregistrements audio fictifs sud-coréens via un appareil étranger¹³⁵⁵.

Le phénomène semble s'accroître malgré une répression de plus en plus forte¹³⁵⁶. Vers la mi-2022, les autorités nord-coréennes reconnaissent à demi-mot l'ampleur prise par la

¹³⁵² Le fait de stocker sur un CD/DVD des biens culturels légalement acquis relève de l'exception « copie privée », et constitue donc une pratique légale ; en revanche, le fait de remettre le CD/DVD à autrui pour lui permettre de consommer ces biens culturels est une pratique illégale, dès lors que cette dernière sort de l'exception « copie à usage privé »

¹³⁵³ HAJEK Danny, « Watching Foreign Movies Is Illegal In North Korea, But Some Do It Anyway », *NPR*, 5 juil. 2017

¹³⁵⁴ PEARSON James, « The \$50 device that symbolizes a shift in North Korea », *Reuters*, 27 mars 2015

¹³⁵⁵ WARD Peter et DENNEY Steven, *Information Dissemination in North Korea: A Report for NGOs*, Rapport pour le National Endowment for Democracy (NED), janv. 2022, p. 11

¹³⁵⁶ Depuis 2015, l'État alourdit les sanctions contre les consommateurs de médias étrangers, après s'être au contraire concentré sur les fournisseurs de biens culturels entre 2009 et 2015. Par ailleurs, les gardes-frontières sont de plus en plus difficiles à soudoyer pour l'obtention de films étrangers. La loi de décembre 2020 sur la dénonciation de la pensée et de la culture réactionnaires punit l'utilisation des polices d'écriture et de l'argot sud-coréens, la distribution massive de films sud-coréens, la consommation de films étrangers (notamment sud-coréens, états-uniens et japonais). Depuis la loi de 2020, ont été exécutés publiquement au moins un vendeur de films étrangers à Wonsan, quatre vendeurs à Pyongyang de vidéos sud-coréennes qu'ils ont distribuées dans tout le pays, ainsi que deux

consommation nord-coréenne de médias étrangers : dans un document adressé à la Ligue de la jeunesse patriotique socialiste, les autorités accusent la distribution et la consommation secrètes d'enregistrements « *étranges et décadents* » d'avoir « *terni une atmosphère sociale saine* »¹³⁵⁷. La consommation nord-coréenne de contenus étrangers est en effet un sujet pris très au sérieux par le pouvoir politique. En 2014, la transfuge Yeonmi Park a déclaré avoir vu le film *Titanic* étant enfant, et que ce film lui avait fait prendre conscience qu'un homme pouvait mourir par amour pour une femme : « *dans la culture nord-coréenne, l'amour est une chose honteuse et personne n'en parle en public. (...) Tous les gens, peu importe leur couleur, leur culture ou leur langue, semblaient se soucier de l'amour en-dehors de nous – pourquoi le régime ne nous a-t-il pas autorisé à l'exprimer ?* »¹³⁵⁸. En 2017, 92% de 350 transfuges, réfugiés et voyageurs nord-coréens déclaraient avoir consommé du contenu étranger sur un lecteur DVD¹³⁵⁹. Jieun Baek, chercheuse à l'Université de Harvard et spécialiste de la Corée du Nord, estime que « *les gens ont soif de savoir ce qu'ils ne savent pas. (...) Il est important de ne pas trop romancer le pouvoir de l'information étrangère. Ce n'est pas à cause de quelques clés USB que la « place de Pyongyang » verra des rassemblement demain. Mais en inondant ce pays d'informations étrangères, il y aura des dissidents, tant dans la pensée que dans l'action, qui émergeront de la société nord-coréenne.* »¹³⁶⁰. En juin 2021, Kim Jong Un reconnaissait que, face à la pénétration sans cesse plus forte des influences étrangères – et notamment sud-coréennes –, la Corée du Nord risque de « *s'émietter tel un mur humide* »¹³⁶¹.

En somme, la feinte par périphérique massivement utilisée en Corée du Nord nous conduit à l'observation suivante : **proportionnellement à la population nationale d'internautes, l'échelle de diffusion de la R-DATA « consommation illicite de biens culturels » est bien supérieure en Corée du Nord** (entre 50% et 80% des internautes nord-coréens d'après les données qu'on a rapportées) **qu'en France** (moins de 25% des internautes français comme on l'a vu plus haut). Surtout, cette R-DATA a des répercussions bien plus graves pour le pouvoir politique nord-coréen que pour celui français. Cette observation signifie aussi que : (i) comme pour les autres configurations de contournement étudiées, le contournement par périphérique peut limiter voire neutraliser l'efficacité des techniques de restriction employées ; (ii) grâce au contournement, **l'échelle de diffusion d'une R-DATA peut continuer de croître et d'atteindre la majorité des internautes même dans un environnement numérique extrêmement restreint** (quasi-impossibilité d'accéder au réseau internet public, filtrage des applications et fichiers téléchargés par les systèmes

adolescents à Hyesen accusés d'avoir regardé et partagé une émission de télévision sud-coréenne. V. WILLIAMS Martyn, « North Korea Intensifies War Against Foreign Influence », *38 North*, 10 nov. 2021 ; HA Yuna, « Four publicly executed in Pyongyang on charges of distributing "illegal video materials" », *Daily NK*, 12 mars 2021 ; « La situation des droits humains dans le monde. Rapport 2022-2023 », *Amnesty International*, 2023, p. 175 ; RYALL Julian, « Why is North Korea 'cracking down' on 'foreign influence' ? », *Deutsche Welle*, 8 juin 2021 ; « North Korea executes teens for distributing foreign films », *Union of Catholic Asian News*, 5 déc. 2022

¹³⁵⁷ MARTIN Bradley K., « North Koreans: Watching foreign movies is "impure" », *Asia Times*, 6 juil. 2022

¹³⁵⁸ THOMPSON Nathan, « "Watching Titanic made me realise something was wrong in my country", says North Korean defector », *The Guardian*, 26 août 2014

¹³⁵⁹ HAJEK D., « Watching Foreign Movies Is Illegal In North Korea, But Some Do It... », préc., *NPR*, 2017

¹³⁶⁰ *Ibid.*

¹³⁶¹ SANG-HUN Choe, « Kim Jong-un Calls K-Pop a "Vicious Cancer" », *The New York Times*, 10 juin 2021

d'exploitation, filtrage de la connexion Wifi dès la carte SIM, brouillage des fréquences hertziennes aux frontières, captures d'écran automatiques par les systèmes d'exploitation...), **malgré une répression particulièrement active** (perquisitions inopinées par la *bowibu* pour inspecter les périphériques dans les foyers, vérifications des smartphones dans l'espace public pour vérifier l'absence d'argot sud-coréen dans les messages envoyés entre nord-coréens¹³⁶²...) **et sévère** (allant jusqu'à l'exécution publique), et **malgré un formatage psychologique très intense de la population par l'État sur plusieurs générations**.

- ***L'affranchissement par périphérique accessoire***

On appelle « affranchissement par périphérique accessoire » la configuration dans laquelle, pour persister à produire ou stocker une R-DATA, le prescripteur numérique se sert d'un périphérique accessoire pour accéder à un autre espace logique une fois la restriction intervenue. La différence avec la feinte par périphérique accessoire réside dans le changement de l'espace logique destinataire une fois intervenue la restriction.

En effet, dans les exemples de la feinte par périphérique accessoire, les utilisateurs ne changeaient pas d'espace logique pour faire exécuter leurs R-DATA une fois intervenue la restriction : le périphérique utilisé peut varier (disque dur externe, CD, DVD, clé USB, carte mémoire...), mais les utilisateurs font exécuter la R-DATA dans le même espace logique local (le système d'exploitation) pour lire un contenu restreint. Qu'il y ait ou non restriction, l'utilisateur lit des vidéos, images, textes et enregistrements audio interdits sur le même espace logique local. En revanche, il y a affranchissement lorsque l'utilisateur change l'espace logique destinataire de ses requêtes une fois intervenue la restriction. Il en va ainsi des Nord-coréens qui utilisent un notel pour consulter illégalement des contenus étrangers : dans ce cas, ils accèdent à un espace logique spécifique (le système d'exploitation du notel) afin d'y faire exécuter leurs requêtes. En l'espèce, le changement d'espace logique destinataire des requêtes est donc le moyen grâce auquel les utilisateurs nord-coréens contournent les restrictions d'accès aux contenus étrangers, et ce changement d'espace logique est permis à l'aide d'un périphérique accessoire. Dès lors, les internautes nord-coréens qui se servent d'un notel pour consommer illégalement des contenus étrangers s'affranchissent par périphérique accessoire des restrictions étatiques.

Un autre exemple de plus en plus répandu d'affranchissement par périphérique accessoire est celui du « jailbreak » en Corée du Nord. Le jailbreak est une méthode qui consiste à exploiter les failles d'un logiciel installé par le fabricant dans le but de remplacer ce logiciel par un autre sur le même appareil. En Corée du Nord, la première motivation de cette pratique semble être la volonté des Nord-coréens de « *contourner la sécurité des téléphones et d'être capables d'installer différentes applications, filtres de photos et des fichiers multimédias qui n'auraient pas été autorisés autrement* »¹³⁶³. Précisément, les utilisateurs chargent sur une clé USB le logiciel destiné à remplacer le système d'exploitation de l'État ; ils branchent ensuite leur clé à leur terminal pour effectuer la substitution. Début 2022, le phénomène semblait récent mais concerner déjà 5% à 10% de la population, et peut-être jusqu'à 30% des étudiants à l'université

¹³⁶² La *bowibu* est la police secrète nord-coréenne placée sous l'autorité du ministère de la sécurité publique. V. HAJEK D., « Watching Foreign Movies Is Illegal In North Korea, But Some Do It... », préc., *NPR*, 2017 ; RYALL J., « Why is North Korea 'cracking down' on 'foreign influence' ? », préc., *Deutsche Welle*, 8 juin 2021

¹³⁶³ WILLIAMS Martyn et SCHIESS Niklaus, « Project Reveal. New research into North Korea's digital control system », *Lumen*, avr. 2022, p. 20

d'après les témoignages de deux transfuges¹³⁶⁴. On peut toutefois envisager que cette pratique continuera à gagner de l'ampleur si des clés USB ou des cartes micro SD stockant un code de jailbreak sont vendues sur le marché noir. En utilisant un code de jailbreak, les internautes nord-coréens peuvent supprimer les barrières posées par la signature électronique, télécharger des applications chinoises de routage (comme Root 方手), et ainsi se connecter au réseau internet international. À l'aide d'un périphérique, les Nord-coréens peuvent ainsi quitter l'espace logique dans lequel ils sont enfermés (systèmes d'exploitation nord-coréens) au profit d'autres espaces logiques (applications hébergées à l'étranger), et donc s'affranchir des restrictions d'accès au réseau internet public.

Les exemples imaginables d'affranchissement par périphérique accessoire sont nombreux. Supposons qu'une utilisatrice bloque l'accès de son profil à un utilisateur qui la harcèle ; ce dernier peut utiliser un objet connecté (tel un drone ou des AirTags¹³⁶⁵) pour surveiller l'utilisatrice et persister à la harceler. Ce faisant, le harceleur s'affranchit par périphérique accessoire du blocage dont il est l'objet pour persister à produire la R-DATA « cyberharcèlement ».

Notre étude sur les configurations de contournement nous permet d'en tirer deux conclusions. D'une part, **toutes les configurations de contournement examinées sont inhérentes au réseau internet** : ces configurations nécessitent une diversité d'espaces logiques disponibles (migration), la capacité de produire différentes données (feinte), l'existence d'intermédiaires (saut, affranchissement) et la présence de périphériques accessoires (feinte et affranchissement par périphérique accessoire), soit des éléments qui sont tous nécessaires au fonctionnement du réseau. Cela signifie qu'un réseau internet national, aussi longtemps qu'il est fonctionnel, peut être utilisé à des fins de contournement – on l'a observé quel que soit le pays (États-Unis, France, Russie, Chine, Corée du Nord), le niveau de restriction mis en œuvre et l'environnement de régulation concerné (libéral, autoritaire, totalitaire). D'autre part, **toutes les configurations de contournement examinées peuvent limiter voire neutraliser l'efficacité des restrictions d'accès** : grâce à la migration, les alt-techs ont gagné davantage d'utilisateurs après la restriction de Parler aux États-Unis, tout comme le réseau social Telegram en Russie une fois restreint ; grâce à la feinte, les utilisateurs chinois amplifient considérablement l'échelle de diffusion de plusieurs R-DATA malgré une censure très réactive et coordonnée ; grâce au saut (notamment à l'aide de VPN), plus de la moitié des utilisateurs russes d'Instagram ont continué à y accéder malgré le blocage ; grâce à l'affranchissement, les marchés noirs en ligne ont vu leur échelle de diffusion croître constamment malgré les suppressions successives et proactives de ces marchés ; grâce à la feinte et à l'affranchissement par périphérique accessoire, la majorité des internautes nord-coréens peut consommer illégalement des contenus étrangers, et une fraction de plus en plus importante peut même accéder au réseau internet public. Cela signifie que, à l'aide du contournement, les prescripteurs numériques peuvent toujours faire échec à l'efficacité d'une technique de restriction sur internet.

¹³⁶⁴ *Ibid.*, p. 21

¹³⁶⁵ Les AirTags sont des objets connectés de la taille d'une pièce de monnaie, développés par Apple et conçus pour aider leur propriétaire à géolocaliser ses affaires. Depuis leur apparition en 2021, les AirTags sont fréquemment glissés dans les poches ou posés sur les victimes pour permettre à leur propriétaire de suivre leurs déplacements. « Harcèlement : cinq questions sur les AirTags, ces "mouchards" d'Apple dont l'usage détourné est dénoncé sur les réseaux sociaux », *France Info*, 14 juin 2023

Paragraphe 2. Le contrôle de l'échelle de diffusion d'une donnée sur internet

On proposera d'abord un modèle théorique pour évaluer systématiquement le risque de contournement que fait courir telle ou telle technique de restriction face à telle ou telle R-DATA (A). On exposera également des méthodes pour limiter le risque de délaissement des techniques par augmentation de l'accès, et on en déduira des propositions pour contrôler l'échelle de diffusion d'une donnée dans le cyberspace (B).

A) Les équilibres de régulation de l'échelle de diffusion d'une donnée en ligne

1. Les motivations des prescripteurs à produire ou stocker des données en ligne

On a défini la régulation juridique de l'échelle de diffusion d'une donnée en ligne comme la méthode : (i) qui consiste à éliminer les problèmes venant perturber cette échelle de diffusion, (ii) en s'appuyant sur des normes juridiques pour contrôler les échanges qu'entretiennent les producteurs de données entre eux sur internet et avec le milieu extérieur à internet, (iii) de façon à orienter cette échelle de diffusion vers un point d'équilibre où se compensent les effets contraires dont le déséquilibre perturbe ladite échelle. Sur le premier élément de la définition, on connaît déjà la perturbation qu'on cherche à éliminer. On cherche à éliminer l'inefficacité d'une norme juridique sur l'échelle de diffusion, c'est-à-dire l'échec d'une telle norme à diminuer l'échelle de diffusion d'une R-DATA ou à amplifier l'échelle de diffusion d'un A-DATA. Sur le deuxième élément de la définition, les techniques de régulation examinées nous ont permis de décrire de nombreuses normes juridiques destinées à contrôler les échanges qu'entretiennent les producteurs de données entre eux sur internet. Reste donc à résoudre le troisième élément de définition : quels sont les effets contraires dont le déséquilibre provoque cette perturbation, cette inefficacité juridique ? Et comment faire varier l'échelle de diffusion d'une R-DATA et d'une A-DATA à l'aide de normes juridiques ?

On cherchera d'abord à répondre à la première question : **quel déséquilibre provoque l'inefficacité des normes juridiques à contrôler l'échelle de diffusion d'une donnée en ligne ?** On sait que les prescripteurs en ligne (fabricant, programmeur, opérateur de transmission, gestionnaire de programmes, administrateur de serveurs et utilisateur) sont les seuls acteurs humains à contribuer directement à l'échelle de diffusion d'une donnée stockée dans le cyberspace, car ce sont les seuls acteurs à pouvoir directement produire ou stocker des données. Par conséquent, dès lors que l'échelle de diffusion d'une donnée est constituée par le nombre de machines qui produisent ou stockent cette donnée, l'échelle de diffusion d'une donnée en ligne varie selon les actions de production ou de stockage des prescripteurs en ligne.

Pour rechercher les causes de l'inefficacité d'une norme juridique à contrôler les variations d'une échelle de diffusion, on se demandera donc ce qui conduit les prescripteurs numériques à rendre inefficace une norme juridique. D'après notre définition de l'efficacité juridique sur l'échelle de diffusion d'une donnée, on a rapporté deux hypothèses dans lesquelles une norme juridique peut être inefficace en la matière :

- Soit les prescripteurs persistent à produire et/ou à stocker une donnée dont le régulateur étatique souhaite réduire l'échelle de diffusion (R-DATA) ;

- Soit les prescripteurs ne produisent ni ne stockent une donnée dont le régulateur étatique souhaite amplifier l'échelle de diffusion (A-DATA).

On cherche d'abord à savoir ce qui conduit les prescripteurs à persister la production ou le stockage de R-DATA. On a vu que le régulateur peut chercher à diminuer l'échelle de diffusion d'une R-DATA soit en agissant directement sur l'accès à cette R-DATA (en restreignant l'accès à cette dernière), soit en agissant indirectement dessus (en augmentant l'accès à une donnée concurrente – par exemple en développant l'offre légale de vidéos et de musiques à la demande pour diminuer l'échelle de diffusion de la R-DATA « consommation illicite de biens culturels en ligne »). Avant d'examiner les techniques d'augmentation de l'accès, on s'intéressera dans un premier temps aux raisons qui peuvent conduire le prescripteur numérique à faire échouer des techniques de restriction.

Face à une technique de restriction de l'accès, le prescripteur peut réagir de deux façons : soit il persiste à produire ou à stocker la R-DATA dont l'accès est restreint ; soit il cesse de la produire ou de la stocker une fois la restriction intervenue. Dans le premier cas, la restriction est inefficace pour empêcher ce prescripteur de contribuer à l'échelle de diffusion de la R-DATA. Dans le second cas, au contraire, la restriction est efficace pour empêcher le prescripteur de maintenir sa contribution à l'échelle de diffusion de la R-DATA, et donc pour réduire cette échelle de diffusion. Prenons l'exemple de la R-DATA « publication et consultation de fausses informations » : si le régulateur étatique ordonne aux hébergeurs de bloquer ou de supprimer de fausses informations, les utilisateurs peuvent soit persister à produire ou à stocker cette R-DATA (auquel cas ils en maintiennent l'échelle de diffusion malgré la restriction), soit cesser de la produire ou de la stocker (auquel cas la restriction réussit à réduire l'échelle de diffusion). De même, outre les utilisateurs, les hébergeurs sont d'autres types de prescripteurs en ligne (gestionnaires d'applications et administrateurs de serveurs) qui peuvent à leur tour accepter de bloquer ou de supprimer les fausses informations à la demande du régulateur, ou bien refuser de le faire et ainsi persister à stocker la R-DATA sur leurs serveurs. Face à une technique de restriction, tous les prescripteurs (utilisateurs, gestionnaires d'applications, programmeurs, fabricants...) impliqués dans l'échelle de diffusion d'une donnée peuvent adopter l'une ou l'autre de ces deux réactions – persister ou cesser la production/le stockage de cette donnée.

Qu'est-ce qui motive les prescripteurs à adopter ces réactions ? On voit deux types de motivations pouvant conduire un prescripteur numérique à stocker ou à produire une donnée en ligne : le prescripteur peut être guidé par une motivation intentionnelle ou accidentelle. On parle de « motivation intentionnelle » lorsque la donnée produite ou stockée par le prescripteur est conforme à la donnée qu'il espérait voir produite ou stockée. Seul le prescripteur individuel est donc à même d'évaluer très exactement si, une fois exécutée, la donnée qu'il a produite ou stockée est conforme à sa volonté. **Le caractère intentionnel ou accidentel d'une motivation s'évalue donc *après* l'exécution d'une donnée**, car le prescripteur ne peut pas évaluer le respect de sa volonté avant que soit exécutée sa requête – sa requête peut en effet engendrer la production ou le stockage d'une donnée contraire à sa volonté comme on le verra. Si la donnée produite ou stockée *après* exécution est conforme à la donnée que le prescripteur voulait produire ou stocker *avant* l'exécution, alors on dira que ce prescripteur est motivé intentionnellement par la production ou le stockage de cette donnée. Ainsi, le prescripteur est guidé par une motivation intentionnelle lorsque le message haineux qu'il produit ou héberge correspond à ce qu'il voulait produire ou héberger *avant* de le faire, lorsque sa consommation illicite d'un bien culturel résulte de la volonté de consommer illégalement/gratuitement un bien

culturel en ligne, lorsqu'il achète effectivement des armes ou des drogues en ligne en ayant préalablement eu l'intention de les acheter etc.

Face à une technique de restriction, deux scénarii peuvent se produire pour le prescripteur intentionnel. D'abord, la motivation du prescripteur peut résister à la technique de restriction, auquel cas la motivation du prescripteur à faire stocker une R-DATA s'élève à un haut degré (motivation tenace) qui justifie pour le prescripteur les efforts voire les risques du stockage de cette R-DATA. On appelle « **attachement intentionnel** du prescripteur (à la donnée produite ou stockée) » ce haut degré de motivation qui conduit le prescripteur à persister le stockage de la donnée malgré la restriction. Inversement, la motivation du prescripteur peut céder face à la restriction, auquel cas la motivation du prescripteur à faire stocker une R-DATA s'élève à un faible degré (motivation fragile) qui ne justifie pas pour le prescripteur les efforts voire les risques du stockage ou de la production de cette R-DATA. On appelle « **détachement intentionnel** du prescripteur (à la donnée produite ou stockée) » ce faible degré de motivation qui conduit le prescripteur à cesser le stockage de la donnée une fois la restriction intervenue. Par conséquent, **le prescripteur intentionnel persiste à produire ou à stocker une R-DATA dont l'accès est restreint s'il est guidé par un haut degré de motivation** (attachement intentionnel du prescripteur à la R-DATA), **et cesse de la produire ou de la stocker lorsqu'il est guidé par un faible degré de motivation** (détachement intentionnel du prescripteur vis-à-vis de la R-DATA). Le degré de motivation intentionnelle est très variable d'un prescripteur à un autre (certains prescripteurs seront plus ou moins attachés ou détachés d'une R-DATA)¹³⁶⁶ mais, aussi variable soit ce degré, toutes les intentions sont rattachables à l'un de ces deux pôles selon qu'elles génèrent une persistance ou une cessation du stockage de la R-DATA face à la restriction.

Quant aux motivations accidentelles, elles se présentent lorsque la donnée produite ou stockée par le prescripteur n'est pas conforme à la donnée qu'il espérait voir produite ou stockée. À nouveau, le caractère accidentel d'une motivation s'évalue après l'exécution d'une donnée : si la donnée produite ou stockée *après* exécution n'est pas conforme à la donnée que le prescripteur voulait produire ou stocker *avant* l'exécution, alors on dira que ce prescripteur est motivé intentionnellement par la production ou le stockage de cette donnée. Il en va ainsi du prescripteur qui espère télécharger un article universitaire ou une photo mais qui, en téléchargeant ainsi ce fichier, stocke sur sa propre machine un logiciel malveillant contenu dans ce fichier ; il en va de même pour le prescripteur qui espère se divertir sur les réseaux sociaux mais qui, sans le vouloir, est exposé à des contenus haineux valorisés par l'algorithme ou présents dans les commentaires ; c'est encore le cas du prescripteur qui partage une fausse information sans savoir qu'elle est fausse, ou de celui qui valide un achat sur internet sans savoir qu'il s'agit d'une escroquerie. Dans tous ces cas, c'est une motivation accidentelle qui pousse le prescripteur à produire ou à stocker une donnée. Une production ou un stockage accidentel résulte d'un manque de contrôle du prescripteur sur la donnée qu'il produit ou stocke (ignorance de la donnée qui sera effectivement produite ou stockée, outils insuffisants pour permettre au prescripteur de restreindre son propre accès à des données indésirables, méconnaissance des signes révélateurs d'un logiciel malveillant...).

¹³⁶⁶ Par exemple, on a rapporté que les consommateurs illicites de biens culturels en ligne avaient en moyenne 1,85 raisons de pratiquer leur consommation illicite en 2022, mais certains d'entre eux ont peut-être 5 raisons différentes de consommer illégalement ces biens culturels tandis que d'autres n'ont peut-être qu'une seule raison ; de même, les raisons de leur consommation sont très importantes pour certains, très relatives pour d'autres

À nouveau, face à une technique de restriction (blocage d'un logiciel malveillant, suppression d'un contenu haineux surexposé, avertissement d'accès à une fausse information...), deux scénarii peuvent se produire pour le prescripteur accidentel. D'abord, la motivation du prescripteur peut résister à la technique de restriction : dans ce cas, le prescripteur persiste à diffuser la R-DATA car la restriction mise en œuvre ne lui permet pas de contrôler pleinement le stockage ni la production de cette donnée. On appelle « **aléa** » ce haut degré de motivation accidentelle qui conduit le prescripteur à persister le stockage ou la production de la donnée malgré la restriction. Inversement, la motivation du prescripteur peut céder face à la restriction : dans ce cas, le prescripteur cesse de produire ou de stocker la donnée une fois la restriction intervenue. On appelle « **incident** » ce faible degré de motivation accidentelle qui conduit le prescripteur à cesser le stockage de la donnée une fois la restriction intervenue. Là encore, aussi variable soit le degré de motivation accidentelle d'un prescripteur à l'autre, toutes les motivations accidentelles sont rattachables à l'un de ces deux pôles – aléa et incident – selon qu'elles génèrent une persistance ou une cessation du stockage de la R-DATA face à la restriction.

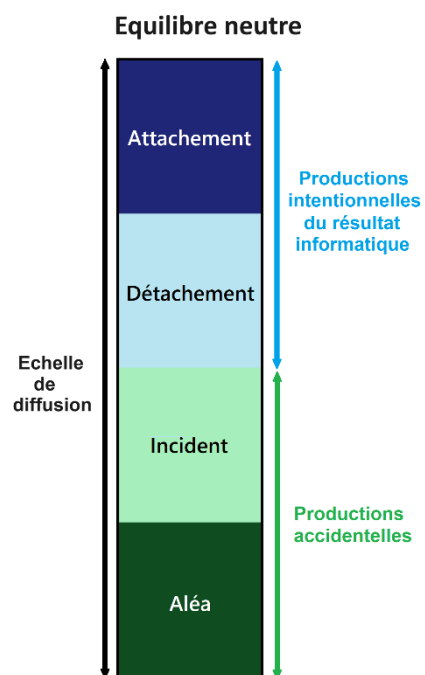
En somme, la réaction des prescripteurs confrontés à une restriction dépend du degré de motivation de chacun de ces prescripteurs. Ils persisteront à produire et à stocker une R-DATA dont l'accès est restreint s'ils sont guidés par un haut degré de motivation intentionnelle (attachement) ou accidentelle (aléa). Ils cesseront de la produire et de la stocker s'ils sont guidés par un faible degré de motivation intentionnelle (détachement) ou accidentelle (incident). Plus le prescripteur est motivé à produire à stocker une donnée, plus fort est le risque qu'il persiste à stocker une R-DATA. Cette présentation des motivations intentionnelles et accidentelles nous permet d'identifier les équilibres de régulation de l'échelle de diffusion d'une donnée qui sont en jeu en présence d'une R-DATA.

2. Le fonctionnement des équilibres de régulation de l'échelle de diffusion d'une donnée en ligne

On a vu qu'une échelle de diffusion est composée de stockages et productions intentionnels (SPINT) et de stockages et productions accidentels (SPACC).

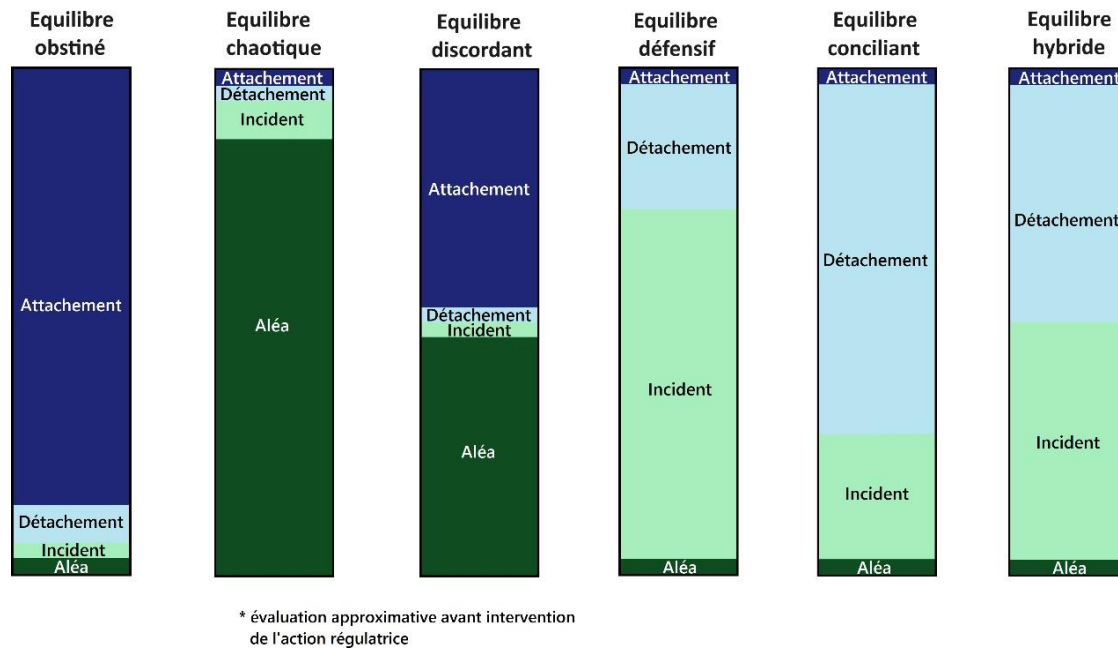
On appellera ainsi « équilibre SPINT/SPACC d'une donnée » la composition de l'échelle de diffusion de cette donnée

selon le ratio productions intentionnelles/accidentelles et selon le ratio haut/faible degré de motivation. En effet, lorsque les prescripteurs produisent ou stockent une donnée, ils alimentent l'échelle de diffusion de cette donnée ; mais tous les prescripteurs qui contribuent à cette échelle de diffusion ne le font pas pour les mêmes raisons. Certains peuvent y contribuer intentionnellement, d'autres accidentellement ; certains peuvent produire ou stocker la donnée par attachement, d'autres par détachement ; certains peuvent produire ou stocker la donnée par aléa, d'autres par incident. Par exemple, on représente ci-contre l'équilibre SPINT/SPACC d'une donnée dont l'échelle de diffusion est composée à 50% de productions et stockages intentionnels (25% d'attachement, 25% de détachement) et à 50% de



productions et stockages accidentels (25% d'incident, 25% d'aléa). Il existe une quasi-infinités

d'équilibres de régulation possibles selon la composition de l'échelle de diffusion, mais on rapporte les standards suivants :



Un équilibre de régulation s'identifie *avant* qu'intervienne l'action régulatrice, de façon à prévoir le risque d'inefficacité d'une technique de régulation et d'envisager la technique la plus appropriée selon l'équilibre concerné. On parle d'équilibre obstiné lorsque l'échelle de diffusion d'une donnée est caractérisée par un très haut degré d'attachement des producteurs à cette donnée. Pour illustrer une R-DATA obéissant à un équilibre obstiné, il en va ainsi probablement de la R-DATA « consultation de contenus pornographiques en ligne par des adolescents ». En effet, on peut supposer que la grande majorité des adolescents qui accèdent à des contenus pornographiques en ligne est attachée à cet accès au point que, face à une restriction frappant cet accès, ils contourneront la restriction pour persister leur accès à la pornographie en ligne. Imaginons que, face à ladite restriction, 90% des adolescents persistent, par attachement, à accéder à de tels contenus : on se trouve dans ce cas en présence d'un équilibre obstiné, et la R-DATA conservera 90% de l'échelle de diffusion qu'elle possédait avant la restriction. Bien sûr, de nombreuses autres communautés en ligne produisent des données dont l'échelle de diffusion obéit à un équilibre obstiné – on a vu le cas de la communauté Gab particulièrement obstinée à produire des contenus haineux, ou des communautés JVC et 4chan particulièrement obstinées à se coordonner pour mener certaines actions malveillantes ou déloyales.

On parlera d'équilibre chaotique si l'échelle de diffusion d'une donnée est caractérisée par un très haut degré d'aléa. Dans ce cas, la donnée acquiert son échelle de diffusion en raison du manque de contrôle des prescripteurs sur la production ou le stockage de cette donnée. Cet équilibre concerne probablement les échelles de diffusion de la plupart des cyberattaques.

Nos schémas qui représentent les équilibres de régulation mettent en relief des parts de couleur foncée (attachement et aléa) et des parts de couleur claire (détachement et incident). Les parts foncées traduisent l'échelle de diffusion qui se maintient après la restriction (par contournement) ; les parts claires traduisent la portion de l'échelle de diffusion qui disparaît une fois la restriction intervenue. On a par ailleurs démontré que malgré la restriction de l'accès à une R-DATA, *tous*

les prescripteurs peuvent *toujours* persister le stockage ou la production de cette donnée grâce au contournement ¹³⁶⁷. Par conséquent, **un équilibre obstiné ou chaotique est toujours possible**. Or, dans la mesure où les parts foncées se maintiennent après la restriction, **une forte baisse de l'échelle de diffusion d'une donnée ne peut être espérée qu'en-dehors d'un équilibre obstiné ou chaotique**. Cela signifie que le régulateur a tout intérêt à transformer des équilibres obstinés et chaotiques en équilibres défensifs ou conciliants pour réduire fortement l'échelle de diffusion d'une R-DATA.

Equilibre SPINT/SPACC de la R-DATA
"accès à Instagram depuis le territoire russe"
en janvier 2022 (avant le blocage de mars 2022)



Avant de voir comment réaliser cette transformation, quel est exactement l'intérêt d'étudier une échelle de diffusion à travers son équilibre SPINT/SPACC ? **L'identification d'un équilibre SPINT/SPACC permet d'estimer**, avant même de choisir la technique de régulation à mettre en œuvre, **le risque d'inefficacité de telle ou telle technique, de telle ou telle norme juridique sur l'échelle de diffusion d'une donnée**. On peut l'illustrer à travers les cas concrets déjà rencontrés dans cette thèse. Examinons par exemple le blocage d'Instagram en Russie après l'invasion de l'Ukraine. On a vu que, avant le blocage d'Instagram par la Russie, Instagram totalisait entre 50 et 60 millions d'utilisateurs russes (soit 40 à 50% des internautes russes). Un mois après que le blocage ait été ordonné en mars 2022, 25% des internautes russes continuaient d'accéder à Instagram ¹³⁶⁸. Dans la mesure où il est nécessaire d'avoir un compte utilisateur pour profiter de l'expérience sur

Instagram, l'accès à Instagram est probablement très majoritairement intentionnel. Dans ces conditions, près de la moitié des utilisateurs d'Instagram en Russie semblent avoir persisté, par attachement, à produire ou à stocker la R-DATA « accès à Instagram sur le territoire russe ». On peut donc considérer que près de la moitié des utilisateurs d'Instagram en Russie ont manifesté un attachement à cette R-DATA bloquée. Dès lors, on peut approximativement représenter, comme on l'a fait ci-contre, l'équilibre SPINT/SPACC de cette R-DATA face à un blocage d'Instagram par les opérateurs russes de transmissions de données (FAI). Par conséquent, si le régulateur russe avait pris conscience d'à quel point les utilisateurs russes étaient attachés à Instagram, s'il avait pris conscience de cet équilibre SPINT/SPACC, il aurait pu en déduire que le blocage d'Instagram aurait provoqué un contournement massif.

On invite alors le régulateur – avant même de décider d'une technique de régulation contre une R-DATA – à évaluer le degré d'attachement et le degré d'aléa des prescripteurs qui stockent cette R-DATA. **Si les prescripteurs semblent très attachés à produire ou à stocker une R-**

¹³⁶⁷ Les configurations de contournement qu'on a relevées sont inhérentes au fonctionnement d'internet, et sont donc continuellement exploitables. On l'a bien sûr vu en Corée du Nord, où plus de la moitié des internautes contournent l'interdiction de consommer des musiques, films et séries TV étrangers malgré des techniques de restriction extrême et un isolement quasi-total du réseau internet nord-coréen.

¹³⁶⁸ Centre Levada, « Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), sur *Levada.ru*, avr. 2023

DATA, ou s'ils manquent considérablement de contrôle sur la R-DATA qu'ils produisent ou stockent, alors il y a un risque élevé que ces prescripteurs contournent les restrictions ; inversement, si les prescripteurs semblent assez détachés de la R-DATA, ou si la restriction d'accès met à la disposition des prescripteurs des moyens de contrôle efficaces sur la production ou le stockage de la R-DATA, alors il y a faible risque que les prescripteurs contournent les restrictions.

Il est possible de se faire une idée globale des degrés d'attachement et d'aléa qui caractérisent l'échelle de diffusion d'une R-DATA, en connaissant l'importance de cette R-DATA pour les prescripteurs intentionnels qui la produisent ou la stockent (attachement) ainsi que l'absence de contrôle des prescripteurs accidentels sur la production ou le stockage de cette R-DATA (aléa). On qualifiera d' « absolue » cette méthode d'évaluation des degrés de motivation des prescripteurs, car elle s'appuie sur une estimation fixe. Par exemple, on a vu que le « précédent Telegram » de 2018 en Russie (hausse continue de l'échelle de diffusion de Telegram malgré un blocage intensif par les opérateurs russes de transmissions de données) semble avoir conduit le régulateur russe à épargner WhatsApp des blocages de mars 2022. En effet, WhatsApp étant l'application la plus utilisée en Russie par le nombre de ses utilisateurs, le régulateur a probablement perçu un attachement des utilisateurs russes à cette messagerie instantanée (équilibre obstiné), et donc un risque élevé de contournement en cas de restriction. L'attachement des utilisateurs russes à WhatsApp peut ainsi se déduire dans l'absolu, grâce au nombre d'utilisateurs de WhatsApp en Russie, au temps qu'ils y consacrent et à la quantité de contenus qu'ils y produisent ou consultent. Ou encore, en France, on a vu que l'échelle de diffusion de la R-DATA « consommation illicite de biens culturels en ligne » a légèrement augmenté depuis 2011 (20% des internautes français accédaient à cette R-DATA en 2011 contre 24% en 2022). Cela laisse à penser que cette R-DATA obéit probablement elle aussi à un équilibre obstiné – les prescripteurs qui contribuent à son échelle de diffusion semblent majoritairement attachés à la production et/ou au stockage de cette R-DATA.

Parallèlement à cette méthode d'évaluation absolue, il est aussi possible – et plus précis – d'adopter une méthode d'évaluation relative des degrés de motivation des prescripteurs. Dans ce cas, les degrés de motivation des prescripteurs ne sont pas tenus pour fixes quelles que soient les circonstances, mais sont évalués par rapport à la technique de régulation employée. Pour le comprendre, on se place du point de vue d'un prescripteur numérique qui utilise Instagram : vais-je ou non cesser de me connecter à Instagram si un jour son accès est restreint ? Tout dépend de la technique de restriction employée, et c'est pourquoi les degrés de motivation varient selon la restriction mise en œuvre. On reprend l'exemple de la R-DATA « consultation d'applications pornographiques par des adolescents », en imaginant que l'échelle de diffusion de cette R-DATA couvre 100 adolescents. Si le régulateur ordonne la mise en œuvre d'un avertissement pour l'accès aux sites pornographiques par des mineurs (avec un message de type « confirmez que vous avez bien 18 ans »), on peut supposer que cet avertissement ne dissuadera pas beaucoup de mineurs, et l'échelle de diffusion pourrait tomber de 100 à 90 ; dans ce cas, on peut estimer l'attachement des utilisateurs à 90% face à la technique mobilisée, et on sera alors probablement en présence d'un équilibre obstiné. En revanche, si le régulateur ordonne l'attribution de clés de chiffrement uniques aux terminaux dont les mineurs sont propriétaires, s'il désigne une ou plusieurs plateformes que doivent emprunter tous les utilisateurs pour accéder à des applications pornographiques, et s'il charge ces plateformes d'empêcher le trafic provenant de clés de chiffrement de mineurs et destiné à des applications pornographiques, alors la technique de restriction employée est bien plus dissuasive ; en supposant que 60

mineurs continuent de consulter des applications pornographiques, on peut estimer l'attachement des utilisateurs à 60% face à cette technique. Les degrés de motivation ne sont donc pas des données fixes, mais variables et relatives selon la manière dont les prescripteurs se positionnent à l'égard de la technique mobilisée¹³⁶⁹. Pour les mesurer avec précision, **les degrés de motivation qui composent une échelle de diffusion peuvent donc être évalués en fonction de l'effet plus ou moins dissuasif de la technique utilisée.** Or, dès lors que la composition d'un équilibre de régulation s'identifie *avant* l'intervention régulatrice, l'effet plus ou moins dissuasif d'une technique doit être évalué de manière *anticipée*. En l'espèce, on peut par exemple anticiper qu'un avertissement sera moins dissuasif qu'un filtrage ou un blocage par clés de chiffrement pour empêcher les adolescents d'accéder à de la pornographie en ligne.

Ajoutons enfin que, s'il peut certes relativiser les degrés de motivation des prescripteurs, le caractère dissuasif d'une technique de restriction est très loin de suffire pour empêcher la formation d'équilibres obstinés ou chaotiques. On a vu ainsi que, en France, les détenus ont très largement accès à internet alors que les prisons sont l'espace dans lequel la législation française restreint le plus l'accès à internet au point de l'interdire. De même, aucun pays ne restreint l'accès internet aux chansons et films étrangers plus que la Corée du Nord ; pourtant, on a constaté que la consommation illicite de biens culturels en ligne est deux à trois fois plus élevée en Corée du Nord qu'en France. Les prescripteurs ont donc persisté à produire et à stocker ces R-DATA (accès à internet dans les prisons en France, consommation illicite de biens culturels en ligne en Corée du Nord), probablement parce que ces R-DATA obéissent à un équilibre obstiné. Par conséquent, **lorsque les prescripteurs sont motivés par un degré élevé d'attachement ou d'aléa dans l'absolu** (*i.e.* indépendamment de la technique de régulation utilisée), **l'intensité et la sévérité de la restriction ne réduisent que minimalement le risque de contournement à long terme**, donc le risque que la R-DATA voit son échelle de diffusion se maintenir ou augmenter. Pour cette raison, l'évaluation absolue des degrés de motivation nous semble préférable en première lecture pour envisager le type de technique de régulation à mettre en œuvre ; l'évaluation relative des degrés de motivation – bien que plus précise – mérite d'être retenue en seconde lecture pour retenir la technique de régulation exactement adaptée.

Pour conclure, on a donc identifié l'attachement, le détachement, l'incident et l'aléa (ADIA) comme étant les quatre effets contraires dont le déséquilibre provoque l'inefficacité des normes juridiques. En d'autres termes, **l'inefficacité d'une norme juridique pour contrôler l'échelle de diffusion d'une donnée en ligne peut s'expliquer par un déséquilibre Attachement / Détachement / Incident / Aléa.** Les situations de déséquilibre extrême (donc de risque élevé d'inefficacité juridique) se présentent avec les équilibres obstinés et chaotiques ; les situations d'équilibre extrême (donc de risque faible d'inefficacité juridique) se présentent avec les équilibres conciliants et défensifs. Dans ces conditions, l'inefficacité d'une norme juridique peut être réduite en corrigeant une échelle de diffusion déséquilibrée (obstinée ou chaotique) pour la mettre à l'équilibre (échelle de diffusion conciliante ou défensive). Dès lors, comment transformer une échelle de diffusion déséquilibrée pour la rendre équilibrée et réceptive aux normes juridiques ?

¹³⁶⁹ Si les degrés de motivation sont variables et relatifs, les parts intentionnel/accidentel sont quant à elles des données évaluable de manière fixe et absolue : leur évaluation ne dépend pas de la technique employée, mais de la conformité de la donnée produite ou stockée à la volonté du prescripteur qui l'a produite ou stockée

B) Propositions théoriques pour contrôler l'échelle de diffusion d'une donnée en ligne

1. Moyens de contrôle et données de substitution

On a vu qu'il est particulièrement difficile de réduire l'échelle de diffusion d'une R-DATA qui répond à un équilibre obstiné, chaotique ou discordant car le risque de contournement est élevé. Dans de telles situations, l'échelle de diffusion d'une R-DATA ne peut être réduite que si la part d'attachement est convertie en détachement et si la part d'aléa est convertie en incident. Tant qu'une telle conversion n'a pas lieu, la R-DATA conserve son échelle diffusion alimentée par l'attachement et/ou l'aléa. On se demandera ici comment il est possible de convertir l'attachement en détachement, et l'aléa en incident.

On étudie tour à tour les stockages et productions accidentels (SPACC) puis ceux intentionnels (SPINT), car ces deux modes de diffusion d'une donnée ne réagissent pas de la même façon aux mêmes techniques de régulation. En effet, les SPINT supposent un contrôle des prescripteurs sur les données qu'ils produisent ou stockent, tandis que les SPACC s'expliquent au contraire par une absence de contrôle des prescripteurs sur les données qu'ils produisent ou stockent. Dès lors, dans le cas des SPACC, adopter une technique de restriction qui ne renforce pas le contrôle des prescripteurs sur les données produites ou stockées aura pour effet de maintenir l'incapacité des prescripteurs à contrôler la production ou le stockage de la R-DATA. Les prescripteurs persisteront donc, accidentellement, à produire ou à stocker la R-DATA faute de moyens de contrôle suffisants. Par exemple, si le régulateur ordonne le filtrage des logiciels malveillants détectés par les opérateurs de transmission, une telle technique de filtrage n'offre qu'aux opérateurs de transmission des moyens de contrôle sur les données produites ou stockées par leurs infrastructures réseau ; mais cette technique de filtrage n'améliore pas le contrôle des autres prescripteurs sur le stockage de logiciels malveillants (utilisateurs, fabricants, gestionnaires d'application, administrateurs de serveurs...). Par conséquent, lorsqu'un logiciel malveillant non détecté passe le filtre des opérateurs de transmission – ce qui est inévitable à cause des configurations de contournement exploitables par les cyberattaquants –, les prescripteurs autres que ces opérateurs ne gagnent pas davantage de contrôle sur le stockage de ce logiciel malveillant, et vont donc persister à produire ou à stocker accidentellement de tels logiciels. De cette façon, si seuls les opérateurs voient leurs moyens de contrôle renforcés, les logiciels malveillants peuvent continuer à acquérir une échelle de diffusion extrêmement vaste auprès des utilisateurs, des fabricants ou encore des administrateurs de serveurs.

On peut aussi illustrer la pertinence des moyens de contrôle avec la diffusion de fausses informations. Cette R-DATA est stockée accidentellement si les prescripteurs qui la consultent, en apprenant la fausseté de l'information, cessaient de la consulter et de la diffuser. Elle est stockée intentionnellement si, une fois connue la fausseté de l'information, les prescripteurs persistaient à la diffuser. En supposant que l'échelle de diffusion des fausses informations est majoritairement accidentelle, il serait alors pertinent de mettre à disposition des prescripteurs qui la diffusent des moyens de contrôle, donc des techniques leur permettant de restreindre le stockage de cette R-DATA. Plusieurs études démontrent en ce sens que la technique d'avertissement est assez efficace pour endiguer la croyance et la diffusion de fausses informations, à condition que les messages avertissant de la fausseté de l'information soient spécifiques à la fausse information en cause, soient aisément visibles aux utilisateurs,

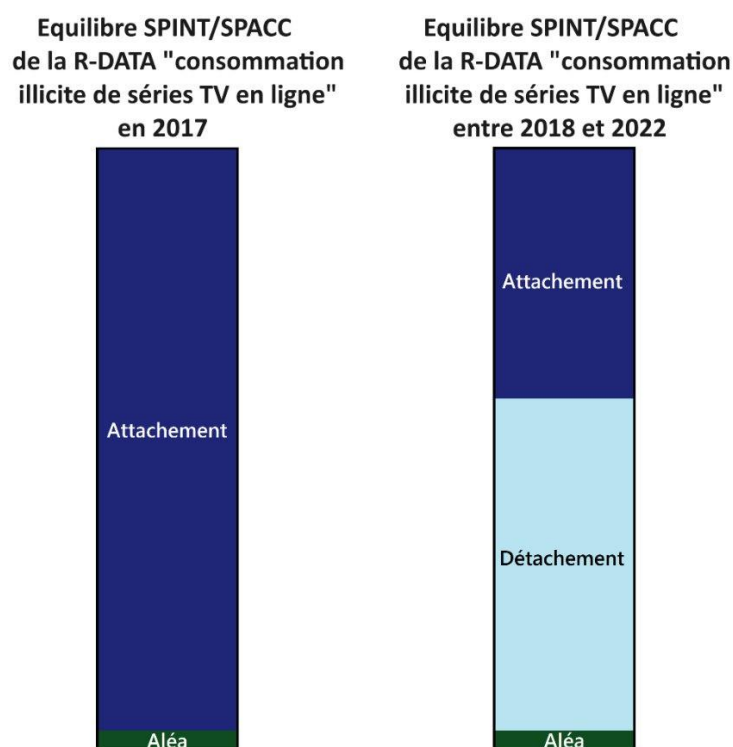
proviennent de sources crédibles telles que des chercheurs, et bénéficient d'une couverture au moins aussi bonne que celle des fausses informations très diffusées¹³⁷⁰.

En revanche, dans le cas des SPINT, les prescripteurs ont pleinement le contrôle sur les R-DATA qu'ils stockent ou qu'ils produisent – c'est d'ailleurs ce contrôle même qui explique leur accès volontaire à une R-DATA. Le fait de renforcer les moyens de contrôle des prescripteurs intentionnels n'aura donc pas pour effet de réduire l'échelle de diffusion d'une R-DATA. Les moyens de contrôle ne sont alors pas d'une grande aide face aux productions et stockages intentionnels de R-DATA. Pour qu'un prescripteur puisse cesser de produire ou de stocker intentionnellement une R-DATA, il lui faut déjà que des A-DATA concurrentes soient disponibles – sans quoi la restriction de cette R-DATA frustrera les besoins du prescripteur sans que ce dernier puisse se rabattre sur un A-DATA. Le risque de contournement d'une telle restriction sera dans ce cas élevé, car le prescripteur ne peut satisfaire ses besoins qu'en accédant à une R-DATA. Par exemple, si des prescripteurs ne peuvent visualiser des films en ligne que de manière illégale, s'il n'existe pas de possibilité légale de regarder des films sur internet, les prescripteurs n'auront tout simplement pas la capacité de satisfaire leurs besoins légalement. De même, si des prescripteurs ne peuvent accéder à leurs réseaux sociaux préférés que de manière illégale, s'il n'existe pas d'offre légale de réseaux sociaux, ces prescripteurs contourneront les restrictions pour accéder aux réseaux sociaux et satisfaire ainsi leurs besoins. **Un prescripteur intentionnel attaché à la production ou au stockage d'une R-DATA ne peut quitter l'échelle de diffusion de cette R-DATA** (consommation illicite de films, accès à des réseaux sociaux illicites) **que si une A-DATA concurrente est disponible** (offre légale de films, de réseaux sociaux).

On a déjà pu illustrer ce phénomène en Chine et en France notamment. En Chine, on a vu que le développement de l'offre légale d'applications chinoises a permis de limiter considérablement le risque que les prescripteurs résidant en Chine (notamment les utilisateurs) contournent les restrictions pour accéder aux applications étrangères illicites. En France, l'essor de l'offre légale de films, de séries TV et de musiques a permis lui aussi provoqué une chute du nombre de prescripteurs qui contournent les restrictions d'accès aux sites illicites de consommation de films, séries TV et musiques. On a vu ainsi que le pourcentage d'internautes en France consommant illégalement des séries TV est passé de 44% à 19% entre 2017 et 2022. Malgré la fermeture ou le blocage des principaux sites web de streaming illégal (Megaupload en 2012, Allostreaming et DPstream en 2013, T411 en 2015, Papystreaming et Sokostream en décembre 2017...) et de téléchargement illégal (ThePirateBay en 2015, Zone-téléchargement, Extratorrent, Torrent8, Isohunt et Cpasbien en décembre 2017...), la part d'internautes en France qui consommait illégalement des séries TV est restée stable à 44% en 2018 comme en 2017. Cela suggère que les mesures de restriction mises en œuvre entre 2012 et 2017 n'ont pas eu d'effet significatif, même à rebours,

¹³⁷⁰ MARTEL Cameron et RAND David G., « Misinformation warning labels are widely effective : A review of warning effects and their moderating features », *Current Opinion in Psychology*, vol. 54, déc. 2023. Pour l'une des premières études sur le sujet, voir celle du MIT : VOSOUGHI Soroush, ROY Deb et ARAL Sinan, « The spread of true and false news online », *Science*, vol. 359, 9 mars 2018, p. 1146-1151. On salue à ce titre le code de bonne conduite de l'UE de 2018, révisé en 2023, par lequel les 34 signataires s'engagent notamment : à fournir aux utilisateurs des outils pour reconnaître, comprendre et signaler la désinformation, accéder à des sources faisant autorité et à des initiatives d'éducation aux médias ; et à signaler aux utilisateurs l'usage de l'IA dans la production d'un contenu. On regrette toutefois l'insuffisance de ce code pour la facilité d'accès aux avertissements (visibilité, concision et synthèse de l'avertissement, affichage immédiat de l'avertissement sur la plateforme...).

sur l'échelle de diffusion de la R-DATA « consommation illicite de films en ligne », et que la quasi-totalité des prescripteurs contribuant à cette échelle de diffusion ont persisté à y contribuer. La réaction des internautes face aux restrictions nous en fait déduire que, en 2017, cette R-DATA était probablement caractérisée par un équilibre obstiné qui rendait son échelle de diffusion très résistante aux techniques de restriction. Cependant, entre 2018 et 2022, la part d'internautes consommant illégalement des séries TV est passé de 44% à 19%, ce qui traduit une chute du nombre d'internautes qui persistent à produire ou à stocker cette R-DATA par attachement. Dans la mesure où la visualisation d'une série TV est généralement intentionnelle (et non accidentelle), on en déduit que les prescripteurs ayant cessé de produire ou de stocker cette R-DATA l'ont fait principalement par détachement (et non par incident). On peut ainsi représenter l'évolution de l'équilibre SPINT/SPACC de cette R-DATA depuis 2017 :



On constate ainsi que, depuis 2017, la part d'attachement a été progressivement convertie en détachement. Or, comment cette conversion a-t-elle opéré ? On a précédemment démontré que l'essor de l'offre légale de vidéos à la demande a eu un rôle causal de premier ordre dans la baisse de la consommation illicite de séries TV. Comme en Chine, le risque de contournement et l'échelle de diffusion de la R-DATA ont effectivement baissé grâce au développement d'une A-DATA concurrente (offre légale de vidéos à la demande). On appelle « donnée de substitution » cette A-DATA concurrente à une R-DATA.

Ainsi, **en présence d'un équilibre accidentel, mieux vaut privilégier les techniques de restriction pour améliorer le contrôle des prescripteurs sur les R-DATA produites ou stockées. En présence d'un équilibre intentionnel, mieux vaut privilégier les techniques d'augmentation pour fournir aux prescripteurs des données de substitution aux R-DATA produites ou stockées.** Les moyens de contrôle donnent aux prescripteurs le pouvoir de quitter une échelle de diffusion à laquelle ils participent accidentellement, et permettent ainsi de convertir l'aléa en incident ; les données de substitution donnent aux prescripteurs le pouvoir de quitter une échelle de diffusion à laquelle ils participent intentionnellement, et permettent

ainsi de convertir l'attachement en détachement. Dès lors, **l'identification de l'équilibre SPINT/SPACC d'une R-DATA permet de connaître la technique de régulation probablement la plus efficace pour réduire l'échelle de diffusion de cette R-DATA** : un équilibre obstiné nécessite de se concentrer sur des techniques de régulation par augmentation, pour déployer des données de substitution ; un équilibre chaotique nécessite de confier aux prescripteurs des moyens de restreindre l'accès à la R-DATA, pour qu'ils puissent contrôler la production ou le stockage de cette R-DATA indésirable ; un équilibre discordant nécessite de jouer tant sur les données de substitution que sur les moyens de contrôle.

Cette théorie est valable quelle que soit l'hypothèse testée jusqu'à présent. Cela nous permet de l'appliquer au-delà des cas examinés en détail dans cette thèse. Concernant les équilibres majoritairement accidentels, prenons l'exemple de la R-DATA « diffusion involontaire de contenus haineux ». Il est en effet fréquent que des utilisateurs consultent, sans le vouloir, des contenus haineux surexposés par les algorithmes des réseaux sociaux – on l'a déjà démontré. Tant que les utilisateurs n'ont pas le contrôle des contenus qu'ils consultent, ils persisteront malgré eux à stocker des contenus haineux et à amplifier leur échelle de diffusion. En appliquant notre théorie, on estime donc indispensable, pour lutter contre la diffusion de contenus haineux, de développer des outils de restriction approfondis à disposition des utilisateurs et d'améliorer ainsi leur contrôle sur le stockage de contenus. Par ailleurs, il est très probable que la R-DATA « diffusion de contenus haineux » obéisse à un équilibre majoritairement accidentelle – mais cela demande à être vérifié –, auquel cas le renforcement de moyens de contrôle des prescripteurs est primordial pour réduire l'échelle de diffusion de cette R-DATA.

Un deuxième exemple est celui de la R-DATA « diffusion involontaire de cyberharcèlement ». On fait ici référence aux victimes de cyberharcèlement qui stockent des messages harcelants en les consultant – il est rare que la lecture de tels messages soient conformes à la volonté du prescripteur qui les lit. Dès lors que cette R-DATA est principalement produite et stockée accidentellement, l'amélioration des moyens de contrôle est appropriée pour réduire son échelle de diffusion. On peut par exemple envisager ce qu'on appellera un « blocage par conversation intelligente » : tout utilisateur d'un réseau social pourrait avoir à sa disposition une intelligence artificielle qui apprendrait à « imiter » la façon de communiquer de l'utilisateur ; lorsque cet utilisateur est victime de cyberharcèlement, il pourrait activer son IA défensive pour qu'elle communique avec le cyberharceleur en imitant le mode d'expression de l'utilisateur ; le cyberharceleur aurait alors le sentiment de discuter avec l'utilisateur, tandis que ce dernier serait totalement désengagé de la conversation et n'en connaîtrait rien ; l'utilisateur peut ainsi laisser le cyberharceleur perdre son temps avec une IA sans connaître les messages du cyberharceleur. Cette technique est évidemment insuffisante à elle seule, mais elle illustre un moyen de contrôle mis à disposition des prescripteurs pour contrôler le stockage de cette R-DATA.

Enfin, concernant la diffusion de logiciels malveillants, on ne saurait faire des propositions aussi complètes et pertinentes qu'un spécialiste de la cybersécurité. Pour autant, on ne doute pas que la baisse de l'échelle de diffusion des logiciels malveillants passe en priorité par le renforcement des moyens de contrôle. La formation de la population aux connaissances de base en cybersécurité et aux signaux d'alerte, la formation officielle de hackers pour améliorer la détection et le traitement des cyberattaques, la recherche spécialisée dans la détection des failles *0-day* (failles d'un produit informatique n'ayant jamais été publiées ni corrigées), l'installation par défaut d'un logiciel antivirus performant, la coordination de la recherche en cybersécurité avec les

opérateurs de transmission de données sont autant de mesures qui améliorent le contrôle des prescripteurs sur le stockage accidentel de *malwares*.

Quant aux équilibres SPINT/SPACC majoritairement intentionnels, on prend pour premier exemple la R-DATA « accès des adolescents à la pornographie en ligne ». Bien que cela mériterait d'être confirmé, on est probablement ici en présence d'un équilibre obstiné. Si on souhaite développer une donnée de substitution qui puisse satisfaire les besoins des adolescents, il importe d'identifier les besoins que les adolescents satisfont en accédant à de tels contenus. Or, compte tenu de la libido des adolescents et de la curiosité pour la découverte du sexe à ce stade de la vie, on doute que les adolescents cesseront de consulter de la pornographie en ligne : l'accès même à ces contenus satisfait leurs besoins sexuels très importants. Par conséquent, la donnée de substitution ne doit pas frustrer ces besoins – sans quoi les adolescents pourraient délaisser cette donnée de substitution et persister leur accès à la R-DATA en contournant les restrictions.

On peut alors envisager d'agir sur deux terrains. Premièrement, le régulateur peut produire, stocker ou promouvoir l'essor d'applications pornographiques légales et réservées aux mineurs. Ces applications pourraient être fréquemment et rigoureusement vérifiées par le régulateur, pour s'assurer que ne sont diffusés que des contenus pornographiques « lissés » – érotisme, contenus non violents, ne représentant pas d'agression sexuelle ni autre infraction etc. Deuxièmement, le régulateur peut compléter ces techniques d'augmentation (donnée de substitution) par des techniques de restriction difficiles à contourner – le chiffrement étant l'une des techniques les plus difficiles à contourner comme on l'a déjà relevé. On a ainsi proposé l'attribution d'une signature électronique aux mineurs qui acquièrent un matériel informatique ; les opérateurs de transmission de données seraient chargés de rediriger tout le trafic reçu (y compris celui provenant de majeurs) vers des plateformes agréées par le régulateur ; ces plateformes filtreraient les données signées électroniquement par un mineur et destinées à des sites pornographiques adultes, afin d'empêcher tout accès à un tel site depuis la machine d'un mineur. Inversement, l'accès aux applications pornographiques réservées aux mineurs ne serait autorisé qu'avec la signature électronique d'un mineur (*i.e.* en utilisant la machine d'un mineur). De cette façon, les adolescents peuvent accéder à des contenus pornographiques qui ne représentent pas l'acte sexuel de manière violente ou non consentie, mais il leur est très difficile d'accéder depuis leur machine à des applications aux contenus plus violents qui leur enseigneraient une approche agressive et irrespectueuse de l'acte sexuel ¹³⁷¹. La méthode qu'on propose ici s'inspire notamment de la Chine, qui a développé des applications de substitution aux applications étrangères (techniques d'augmentation) tout en restreignant sévèrement l'accès aux applications étrangères (techniques de restriction). La restriction n'est dans ce cas pas la méthode principale : elle accompagne les techniques d'augmentation et améliore leur efficacité en encourageant l'accès des prescripteurs aux données de substitution. L'accès des adolescents à la pornographie répondant d'un équilibre obstiné, l'efficacité régulatrice dépend principalement de la qualité des données de substitution.

Dans le même sens, la R-DATA « accès à des contenus pédopornographiques » résulte elle aussi probablement d'un équilibre obstiné. Théoriquement, les données de substitution seront

¹³⁷¹ Précisons que l'éducation des mineurs à des rapports sexuels consentants et respectueux ne peuvent évidemment pas reposer sur cette seule technique de régulation, et dépasse le champ du réseau internet

donc les mesures les plus appropriées pour convertir l'attachement en détachement, et ainsi réduire l'échelle de diffusion de cette R-DATA. On propose ainsi, comme au Japon, de rendre légale la diffusion sur internet d'images de synthèse représentant de « faux » enfants ou adolescents créés par logiciel (y compris par IA)¹³⁷² ; de cette façon, les prescripteurs pédophiles pourront se rabattre sur de telles images de synthèse au lieu de consulter des images représentant de vrais enfants et adolescents abusés sexuellement et donc de contribuer économiquement à une mafia qui exploite la sexualité des mineurs en ligne. À nouveau, il nous est indispensable d'accompagner ces données de substitution par des restrictions sévères frappant l'accès aux contenus pédopornographiques représentant de vrais mineurs.

Pour conclure, ajoutons qu'il ne suffit pas de promouvoir des moyens de contrôle ou des données de substitution pour que ces méthodes soient efficaces. En premier lieu, **l'efficacité d'un moyen de contrôle dépend de la mesure dans laquelle ce moyen couvre les lacunes de contrôle des prescripteurs qui produisent ou stockent accidentellement une R-DATA. L'efficacité d'une donnée de substitution dépend de la mesure dans laquelle cette donnée couvre les besoins des prescripteurs qui produisent ou stockent intentionnellement une R-DATA.** Si les moyens de contrôle et les données de substitution, respectivement, ne couvrent pas les lacunes de contrôle des prescripteurs ni leurs besoins, les prescripteurs délaisseront ces moyens et données mis à leur disposition, voire persisteront à contourner les restrictions d'accès aux R-DATA. En somme, pour réduire le risque de contournement et le risque de délaissement, le régulateur doit : donner aux prescripteurs accidentels des outils performants pour se défendre via des moyens de contrôle ; et satisfaire les besoins des prescripteurs intentionnels au moyen de données de substitution. Sur ce dernier point, en examinant le succès des Géants d'internet et des applications chinoises, on recense plusieurs moyens qui peuvent fortement contribuer à satisfaire les besoins des prescripteurs, tels que : le volume d'investissements consacrés à la R&D et la recherche fondamentale par les entreprises du secteur numérique et/ou par la puissance publique, l'innovation et la fédération d'usages déjà largement adoptés, l'ouverture du marché, les circonstances exceptionnelles, l'organisation structurée de programmes/planifications à long terme... On identifie deux grandes variables pour évaluer le risque de délaissement : la valeur ajoutée apportée par la A-DATA aux prescripteurs par rapport à celle de la R-DATA concurrente (plus la valeur ajoutée apportée par la R-DATA aux prescripteurs est supérieure à celle de la A-DATA, plus le risque de délaissement est élevé ; inversement, plus la valeur ajoutée de la A-DATA est supérieure à celle de la R-DATA, plus le risque de délaissement est faible) ; et le volume national de prescripteurs qui accède à une A-DATA par rapport à celui qui accède à une R-DATA concurrente (plus la R-DATA rassemble un grand nombre de prescripteurs, plus l'effet de réseau jouera en sa faveur au détriment de la A-DATA concurrente ; inversement, plus la A-DATA rassemble un grand nombre de prescripteurs, plus l'effet de réseau jouera en sa faveur au détriment de la R-DATA concurrente).

En second lieu, **l'efficacité d'une technique de régulation est conditionnée par le fait que cette technique embrasse le périmètre d'une R-DATA/A-DATA.** Si la technique de régulation dépasse le périmètre de la R-DATA ou A-DATA, ou bien si elle ne couvre pas complètement ce périmètre, elle engendrera un risque d'inefficacité dans la mesure du dépassement ou de la non-couverture du périmètre. Imaginons par exemple une législation qui, dans le but d'interdire tout contact entre majeurs et mineurs établi à des fins sexuelles, de

¹³⁷² L'interdiction de la diffusion d'images pédopornographiques de synthèse est posée par l'art. 9, 2, c) de la Convention sur la cybercriminalité (Convention de Budapest) du 23 novembre 2001. Plusieurs États ont toutefois émis des réserves sur cette disposition – Japon, États-Unis, Royaume-Uni...

séduction et/ou d'exploitation, imposerait une clôture virtuelle sur les réseaux sociaux qui empêcherait toute forme de contact entre les mineurs et les majeurs. Une telle clôture virtuelle dépasserait le périmètre de la R-DATA « contacts entre majeurs et mineurs menés à des fins sexuelles, de séduction et/ou d'exploitation ». Les mineurs qui souhaitent contacter des majeurs à d'autres fins que des fins sexuelles, de séduction et/ou d'exploitation, et les majeurs qui souhaitent contacter des mineurs à d'autres fins que celles-ci, seront alors amenés à contourner la clôture virtuelle. Ladite clôture ainsi contournée ne protégerait donc plus les mineurs contre les contacts établis entre majeurs et mineurs à des fins sexuelles, de séduction et/ou d'exploitation, et l'échelle de diffusion de la R-DATA pourra être maintenue. Inversement, si la clôture virtuelle empêche seulement les contacts établis à des fins sexuelles et d'exploitation de mineurs, elle ne couvre pas les contacts noués à des fins de séduction. Un majeur pourrait alors séduire un mineur sur un réseau social, lui proposer sur le réseau social une rencontre non sexuelle avec le mineur, puis pratiquer avec ce mineur des activités sexuelles lors de la rencontre. Dans ce cas, la clôture virtuelle ne couvrirait pas le périmètre de la R-DATA, et s'expose donc à un risque élevé d'inefficacité.

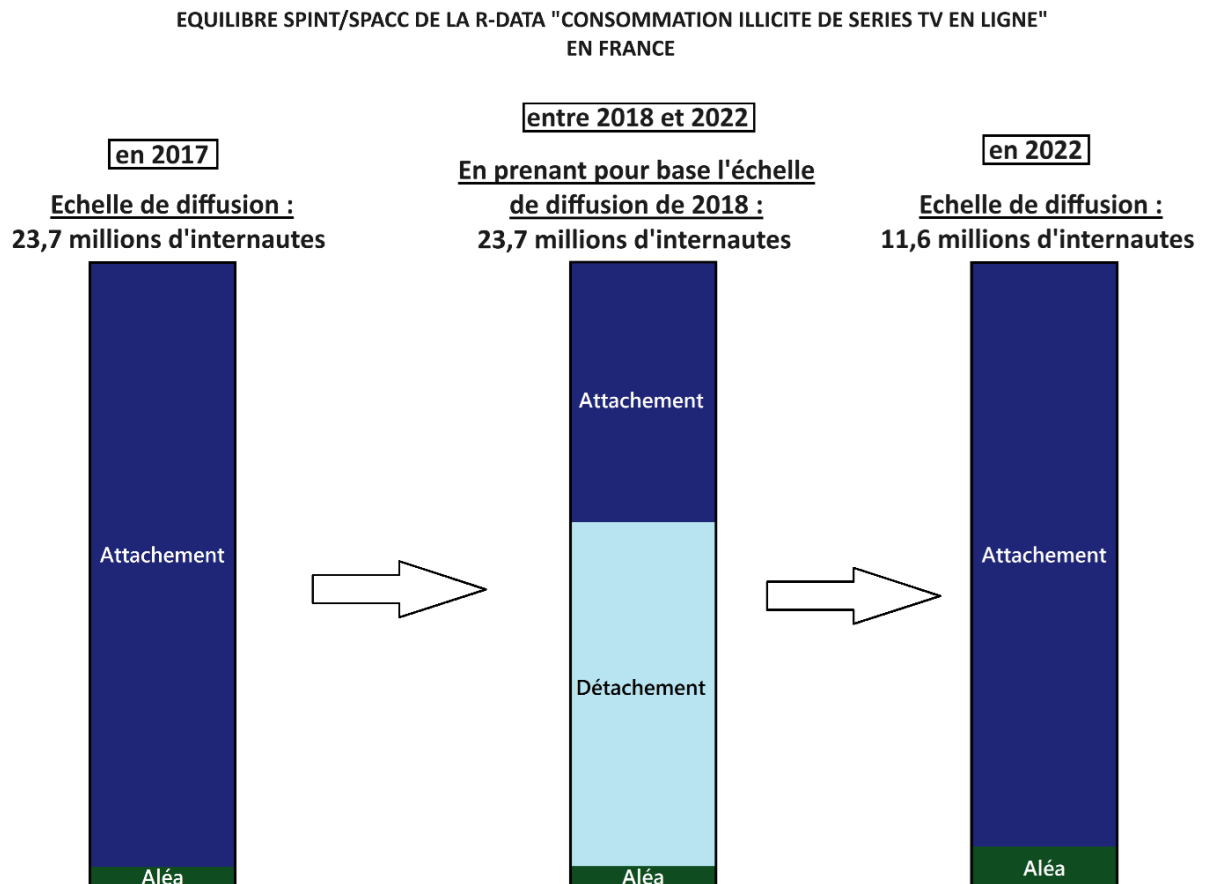
2. Les cycles de régulation

On a vu que l'échelle de diffusion d'une R-DATA peut comporter deux types de parts : une part cédante (détachement et incident) ; et une part résistante (attachement et aléa). Lorsque l'équilibre SPINT/SPACC d'une R-DATA est caractérisé par une part résistante très vaste, il est par définition très difficile (voire quasi-impossible à long terme) de réduire l'échelle de diffusion de cette R-DATA sans modifier son équilibre SPINT/SPACC. On a vu comment modifier l'équilibre SPINT/SPACC d'une R-DATA – en convertissant l'attachement en détachement grâce à l'offre légale de données de substitution, et en convertissant l'aléa en incident grâce à des moyens de contrôle. Une fois la part résistante convertie en part cédante, cette part disparaît de l'échelle de diffusion de la R-DATA.

Dans le cas de la consommation illicite de biens culturels, on a vu que l'offre légale de vidéos à la demande a permis de modifier l'équilibre SPINT/SPAC de la R-DATA « consommation illicite de séries TV ». Or, que se passe-t-il lorsque l'attachement est converti en détachement, ou lorsque l'aléa est converti en incident ? Les parts ainsi converties *quittent* l'échelle de diffusion de la R-DATA, donc ne figurent plus dans l'équilibre de cette échelle de diffusion. Dès lors, **après que la conversion eut opéré, l'échelle de diffusion de la R-DATA se libère de ses parts de détachement et d'incident, donc replonge dans des équilibres obstinés, chaotiques ou discordants car seules demeurent les parts d'attachement et d'aléa** – les parts qui ont résisté à l'action régulatrice.

Certes, la R-DATA regagne son équilibre obstiné, chaotique ou discordant. Mais elle n'a pu le faire qu'en perdant une partie de son échelle de diffusion – celle qui a été convertie en détachement ou en incident. Plus la part résistante convertie en part cédante est importante, plus l'échelle de diffusion est réduite à cette occasion. Pour rester sur notre exemple de la consommation illicite de séries TV en ligne, 44% des 53,8 millions d'internautes en France s'adonnaient à cette pratique en 2017, soit 23,7 millions d'internautes ; en 2022, ils n'étaient plus que 19% parmi les 60,92 millions d'internautes en France, soit 11,6 millions de consommateurs illicites. 12,1 millions d'utilisateurs se sont donc détachés de cette R-DATA (23,7 - 11,6 = 12,1). Une fois partis ces 12 millions d'utilisateurs, ne restent plus que les 11,6 millions de consommateurs illicites qui persistent à produire ou à stocker cette R-DATA par

détachement ou par aléa. Ladite R-DATA obéit donc à un équilibre obstiné en 2022 comme en 2017, mais son échelle de diffusion a été divisée par deux entre 2017 et 2022.



La réduction d'une échelle de diffusion se produit donc par « à-coups » : grâce aux données de substitution, l'échelle de diffusion de la R-DATA est passée de 23,7 millions d'internautes à 11,6 millions entre 2018 et 2022 ; en raison de ce départ des utilisateurs détachés, la R-DATA n'est plus produite et stockée que par attachement ou par aléa, ce qui la plonge à nouveau dans un équilibre obstiné en l'espèce ; il sera alors à nouveau possible de convertir l'attachement en détachement grâce à l'amélioration des données de substitution, ce qui réduira une fois de plus l'échelle de diffusion de la R-DATA (par exemple à 5 millions d'internautes en 2027) ; et ainsi de suite jusqu'à ce que l'échelle de diffusion se tasse totalement, ou jusqu'à ce qu'elle devienne majoritairement accidentelle (auquel cas le renforcement des moyens de contrôle devra être privilégié).

Le fait de réduire l'échelle de diffusion d'une R-DATA implique donc un retour constant de cette échelle de diffusion vers des équilibres chaotiques, obstinés et discordants, et donc un effort constant de conversion des parts résistantes en parts cédantes pour continuer à réduire cette échelle. La régulation de l'échelle de diffusion d'une R-DATA nous semble alors cyclique : l'échelle de diffusion d'une R-DATA ne peut être durablement réduite que par vagues, d'abord en faisant gagner à l'équilibre de cette R-DATA des parts cédantes qui quitteront cette échelle de diffusion (1^{ère} vague d'élimination d'une partie de l'échelle de diffusion), puis en lui faisant gagner de nouvelles parts cédantes (2^e vague d'élimination), et cætera jusqu'à réduction de l'échelle de diffusion au minimum de productions et de stockages résistants. Le travail du régulateur n'est jamais fini : il doit éternellement s'efforcer d'améliorer les données de substitution et les moyens de contrôle, tout en dissuadant l'accès des

prescripteurs à des R-DATA (notamment grâce à des restrictions d'accès à cette R-DATA). On ne voit donc pas une technique précise qui mettrait définitivement un terme à l'échelle de diffusion d'une R-DATA : les données de substitution doivent régulièrement être améliorées et adaptées aux besoins des prescripteurs, tout comme les moyens de contrôle doivent être régulièrement renforcés et adaptés aux raisons qui conduisent les prescripteurs à produire ou à stocker accidentellement une R-DATA.

Pour conclure, à la question « **comment contrôler l'échelle de diffusion d'une donnée sur internet** », on y apporte la réponse suivante : **en satisfaisant les besoins des prescripteurs de manière sécurisée, en leur donnant les moyens d'empêcher la production ou le stockage accidentel de données, et en restreignant l'accès aux R-DATA plus ou moins sévèrement selon le degré d'attachement ou d'aléa**. Si un régulateur souhaite réduire l'échelle de diffusion d'une R-DATA, on l'invite donc à respecter les sept étapes suivantes :

1° / Identifier si la R-DATA est caractérisée par une échelle de diffusion majoritairement intentionnelle ou accidentelle : cela permet au régulateur de déterminer si doit être privilégié le développement de données de substitution, ou bien de moyens de contrôle, ou bien les deux simultanément ;

2°/ Identifier les degrés de motivation des prescripteurs qui contribuent à l'échelle de diffusion de la R-DATA : cela permet au régulateur de déterminer les efforts qui doivent être fournis pour réussir à convertir l'attachement en détachement et l'aléa en incident ;

3°/ Choisir des techniques de régulation qui couvrent exactement le périmètre de la R-DATA sans le dépasser : cela permet au régulateur d'éviter un risque d'inefficacité par contournement (si le périmètre est dépassé par les techniques) ou par accès non-restreint à la R-DATA (si le périmètre n'est pas couvert par les techniques) ;

4°/ Développer des données de substitution légales qui combler la demande et/ou des moyens de défense qui combler les lacunes de contrôle des prescripteurs sur le stockage de données : cela permet au régulateur d'éviter un risque d'inefficacité par délaisement des techniques d'augmentation et par contournement des techniques de restriction ;

5°/ Adopter des techniques de restriction intenses si les données de substitution combler la demande, si la part d'attachement est excessivement tenace ou, dans le cadre de moyens de contrôle, si la part d'aléa est très importante : cela permet au régulateur de pousser les prescripteurs attachés à une R-DATA vers des données de substitution déjà bien développées, de réduire au minimum la part d'attachement, ou d'améliorer l'efficacité des moyens de contrôle pour restreindre le stockage de R-DATA indésirables ;

6°/ Mettre les données de substitution et/ou les moyens de contrôle à disposition des prescripteurs qui contribuent le plus à une échelle de diffusion : cela permet au régulateur d'obtenir la plus large réduction de l'échelle de diffusion d'une R-DATA ;

7°/ Adapter régulièrement les techniques employées aux évolutions de l'équilibre SPINT/SPACC de la R-DATA : cela permet au régulateur d'assurer une baisse continue de l'échelle de diffusion, de façon que cette baisse se poursuive sans s'arrêter à la première vague d'élimination.

Cette méthode de régulation qu'on propose nous semble valable quelle que soit la R-DATA concernée. Elle nous semble d'ailleurs adaptable à la plupart des civilisations culturelles dans le monde (si ce n'est toutes) : n'importe quelle donnée de substitution peut efficacement convertir l'attachement en détachement si elle satisfait et sécurise les besoins des utilisateurs davantage que la R-DATA concurrente, tout comme n'importe quel moyen de contrôle peut efficacement convertir l'aléa en incident s'il couvre les lacunes de contrôle des prescripteurs sur la production ou le stockage accidentel de la R-DATA. **Le régulateur peut donc contrôler efficacement l'échelle de diffusion d'une R-DATA en adoptant n'importe quelle donnée de substitution ou n'importe quel moyen de contrôle conformément à son ordre juridique, à ses objectifs et à ses valeurs morales, pourvu que ces données et moyens de contrôle satisfassent les conditions décrites.** *A priori*, cette méthode de régulation permet donc de créer des normes juridiques qui réduisent efficacement l'échelle de diffusion d'une R-DATA tout en respectant les droits et libertés fondamentaux en Occident, ou en respectant la culture juridique de la régulation en Chine.

L'efficacité de la régulation peut par ailleurs être accrue en décomposant une R-DATA pour agir sur les différentes R-DATA qui la composent. Prenons l'exemple du *grooming*, cette pratique qui consiste pour des majeurs à séduire des mineurs à des fins sexuelles et/ou d'exploitation des mineurs. Ici, la R-DATA réside dans les « contacts de mineurs par des majeurs à des fins sexuelles et/ou de séduction et/ou d'exploitation » (R-DATA 0). Cette R-DATA 0 se décompose elle-même en deux R-DATA : la « production par des majeurs de messages destinés aux mineurs à des fins sexuelles et/ou d'exploitation de mineurs » (R-DATA 1) ; et le « stockage par des mineurs de tels messages produits par des majeurs » (R-DATA 2). La R-DATA 1 est probablement majoritairement intentionnelle – les majeurs qui contactent des mineurs à des fins sexuelles et/ou d'exploitation le font probablement intentionnellement. D'après notre théorie, l'échelle de diffusion de la R-DATA 1 pourra donc être réduite en travaillant sur des données de substitution mises à disposition des majeurs. En revanche, la R-DATA 2 est probablement majoritairement accidentelle : la majorité des mineurs qui reçoivent de tels messages produits par des majeurs ne désire probablement pas les recevoir. L'échelle de diffusion de la R-DATA 2 pourra donc être réduite en améliorant et en intensifiant les moyens de contrôle mis à disposition des mineurs pour restreindre le stockage accidentel de ces messages¹³⁷³. En décomposant la R-DATA 0, on peut donc agir doublement sur la R-DATA 1 (données de substitution mises à disposition des majeurs) et sur la R-DATA 2 (moyens de contrôle mis à disposition des majeurs) pour réduire efficacement l'échelle de diffusion de la R-DATA 0.

Enfin, notre théorie sur les équilibres SPINT/SPACC nous semble proposer suffisamment de paramètres (échelle de diffusion, équilibre majoritairement intentionnel/accidentel, degrés de motivation, méthode d'évaluation absolue ou relative des degrés de motivation, facteurs contribuant au succès d'une A-DATA concurrente...) pour élaborer un algorithme capable de prévoir approximativement les risques de contournement et de délaissement d'une technique de régulation mise en œuvre contre une R-DATA particulière. Nous n'avons malheureusement pas eu l'occasion ni le temps de développer un tel algorithme, mais invitons les chercheuses et chercheurs intéressés par notre travail à explorer cette piste.

¹³⁷³ C'est, entre autres, ce que propose le *Kids Only Safety Act* américain, qui oblige les services de réseaux sociaux à fournir à l'utilisateur mineur des outils pour limiter la capacité des personnes n'ayant aucun lien avec lui à le contacter ou à le trouver sur internet et pour empêcher les tiers de consulter ses données personnelles

CONCLUSION

On ne pourra pas ici résumer la totalité des conclusions tirées dans le cadre de cette thèse, mais on dressera les principales. On classera ces conclusions par thématiques.

1/ La réalité prescriptive du cyberspace

On a démontré que le cyberspace (*i.e.* l'espace mémoire formé par l'ensemble des mémoires informatiques connectées à internet) héberge des règles propres. Ces règles ne sont pas connues des lois électriques, physiques ou mécaniques. Elles ne sont connues que dans le cyberspace, elles ne sont connues que stockées par des machines numériques connectées à internet. On a appelé ces règles des « prescriptions numériques ». Elles peuvent être issues d'instructions rédigées en langage machine ou d'instructions logicielles (prescriptions « abstraites » dans les deux cas, car applicables indépendamment de la survenance d'un cas concret), ou peuvent être issues de requêtes d'accès (prescriptions « concrètes » car applicables uniquement lors de la survenance d'un cas concret).

Non seulement ces prescriptions numériques ne sont connues que du cyberspace, mais elles ont aussi leur propre mode de validation. Ces règles sont en effet validées par interopérabilité, sans que l'exécutant (*i.e.* le processeur de la machine) puisse y insérer sa propre appréciation ni créer lui-même de telles prescriptions, sachant que l'exécutant et l'applicateur de la règle ne font qu'un et que la validation par l'exécutant d'une prescription numérique est liée par la validité de la requête d'accès qui porte cette prescription. On a vu que toutes ces caractéristiques sont fondamentalement contraires au mode de validation des règles de droit. On a vu aussi que ces caractéristiques garantissent à la prescription numérique une effectivité plus forte dans le cyberspace que l'effectivité dont peuvent bénéficier les règles de droit dans l'ordre juridique. Cette effectivité confère un pouvoir d'action considérable aux producteurs de données sur internet (« prescripteurs en ligne ») pour faire exécuter les règles qu'ils souhaitent voir appliquées dans le cyberspace.

Cette thèse a par ailleurs démontré que, outre ce mode de validation des règles tout à fait spécifique, le cyberspace est caractérisé par son propre mode de production des prescriptions — théoriquement ouvert à tous les êtres humains de façon égale, sans que l'exécutant hiérarchise les prescripteurs en ligne ou les prescriptions numériques (autrement que par le caractère prioritaire ou non des requêtes dans un cas concret). Enfin, les prescriptions numériques possèdent leur propre mode d'ordonnancement, c'est-à-dire leur propre mode d'interactions pour fournir son contenu au cyberspace. Ce mode d'ordonnancement est à la fois ubiquitaire (toutes les prescriptions numériques sont disponibles quelle que soit la machine depuis laquelle on y accède, quelle que soit la machine qui les produisent) et diffusible (une même prescription numérique peut contraindre plusieurs machines, sur la base de quoi les données dont une prescription numérique ordonne le stockage peuvent gagner une échelle de diffusion auprès des autres processeurs exécutants membres du réseau).

Sur ces considérations, on a qualifié le cyberspace de « réalité prescriptive », c'est-à-dire un espace qui accueille ses propres prescriptions, et qui est caractérisé par ses propres modes de production, d'exécution et d'ordonnancement des prescriptions. Une concurrence peut se jouer entre plusieurs réalités prescriptives comme on l'a soulevé, y compris entre le cyberspace et l'ordre juridique (autre réalité prescriptive). Cette concurrence se joue notamment sur l'influence qu'exercent les prescriptions (numériques ou étatiques) sur les comportements d'une même population, ou encore sur l'irrespect des normes juridiques par les prescriptions numériques, ou

inversement sur les restrictions d'accès aux prescriptions numériques par les normes juridiques. Cette concurrence s'accompagne d'une complémentarité de ces deux réalités prescriptives, par laquelle le cyberspace contribue à l'efficacité de certaines normes juridiques, et l'ordre juridique s'appuie de plus en plus sur le cyberspace pour faire appliquer ses normes.

2/ Remise en cause de la théorie *Code Is Law*

On a démontré que la théorie *Code Is Law* échoue à expliquer le pouvoir de contrainte qu'exerce l'utilisateur et les opérateurs de transmission de données sur la compréhension machinale, ainsi l'existence d'une source commune à la contrainte exercée par le programmeur et à celle exercée par l'utilisateur (et les opérateurs). En retenant le code binaire (et non le code source) comme l'origine de toute contrainte endogène au cyberspace, on parvient à expliquer des rapports de force interhumains en ligne ignorés par l'explication *Code is Law*.

Retenir le code binaire comme l'origine de la contrainte interne au cyberspace nous a conduit à identifier six catégories de prescripteurs numériques - *i.e.* six catégories de producteurs humains de données binaires (utilisateur, programmeur, fabricant, opérateur de transmission, administrateur de serveur, gestionnaire d'application) -, et à qualifier le code binaire de « bien commun » - de sorte que le pouvoir de prescrire dans le cyberspace est inappropriable. À la fois inappropriable, construit collectivement par tous les prescripteurs numériques, et constitutif d'une réalité prescriptive, le cyberspace est-il ingouvernable par les États, voire menace-t-il leur existence ?

3/ Souveraineté étatique et cyberspace

Nous n'avons identifié aucune menace directe que ferait peser le cyberspace sur l'existence des États et des ordres juridiques. Certes, le contexte social contemporain qui repose sur l'usage croissant des réseaux numériques a probablement une influence sur la conception psychologique des règles de droit qu'ont les juristes, les juges, les avocats et les législateurs. Il est tout à fait possible (mais cela reste à démontrer) que ce contexte social ait incité les juristes à concevoir les normes juridiques de moins en moins comme une « pyramide » des normes et de plus en plus comme un « réseau » de normes. Ce dernier mouvement semble d'ailleurs coïncider avec l'après-seconde guerre mondiale - soit au moment du développement des premiers réseaux numériques -, et s'est intensifié depuis les années 1980-1990 - soit au moment de l'essor des réseaux numériques¹³⁷⁴. Cependant, ce n'est pas le cyberspace lui-même qui étiole la pyramide des normes mais, au mieux, l'influence du contexte social sur les juristes qui pratiquent le droit.

Par ailleurs, et surtout, le développement d'un modèle de normes « en réseau » n'a pas, à notre connaissance, remis en cause la hiérarchie des normes comme la « base » pour résoudre les conflits de normes : les normes constitutionnelles sont toujours supérieures aux normes législatives, qui sont toujours supérieures aux normes réglementaires. Il existe certes des exceptions, qu'on n'a pas trouvées en grand nombre et dont on doute qu'elles soient nettement plus nombreuses aujourd'hui qu'elles l'étaient dans les années 1960-70. Le réseau de normes ne nous semble donc pas avoir chassé la pyramide des normes, mais s'appliquer à des hypothèses différentes : le réseau de normes est généralement utilisé dans les hypothèses où deux normes de même valeur juridique (deux lois, deux normes constitutionnelles, deux actes réglementaires) entrent en conflit, ou dans des hypothèses où le juge voire le législateur

¹³⁷⁴ BARRAUD Boris, *Le droit postmoderne. Une introduction*, L'Harmattan, 2017

recherchent des inspirations dans le corpus juridique (français ou parfois étranger) ; la pyramide des normes est utilisée, comme elle l'a toujours été, dans l'hypothèse où deux normes de valeur juridique différente entrent en conflit.

Au-delà de la hiérarchie des normes - que le cyberspace ne nous semble donc pas menacer directement -, il est en revanche plus probable que le cyberspace ait largement influencé les appels à une démocratie plus participative, et la production à son tour plus participative de certaines normes juridiques. On a vu par exemple que l'ex-secrétaire d'État au numérique, Axelle Lemaire, a soumis la loi pour une République numérique aux amendements déposés en ligne par les citoyens français, tout comme l'Administration du Cyberspace de la Chine soumet fréquemment ses avis et règlements aux amendements des citoyens chinois via internet. En effet, d'une part, en tant que bien commun et réalité prescriptive, le cyberspace est un espace construit collectivement par des règles dont n'importe quel utilisateur peut obtenir l'exécution immédiate. D'autre part, une très large partie de la population est désormais présente dans le cyberspace. Un État absent du cyberspace, ou qui ne s'adapte pas aux capacités participatives que fournit internet, peut craindre d'être dépassé par les progrès sociaux et donc délégitimé par sa population.

Tant que les règles de droit fournissent à la population des avantages différents des prescriptions numériques, l'État restera légitime pour les bénéfices qu'il est le seul à pouvoir apporter à sa population. Plus préoccupante est la situation dans laquelle les prescriptions numériques apportent à cette population les mêmes avantages, voire de meilleurs avantages, que les règles de droit. Par exemple, les prescriptions numériques en ligne peuvent permettre : de régler des achats et des ventes sans recourir aux monnaies contrôlées par les États (par cryptomonnaies, NFT...) ; de solliciter sur internet des services d'enquête qui se substituent aux services de police ; de solliciter une intelligence artificielle en ligne pour résoudre un litige de droit... Les normes juridiques doivent apporter à la population d'un État des avantages différents, voire de meilleure qualité, que ceux proposés par les prescriptions numériques issues de sources privées. On voit deux moyens pour cela : l'encadrement juridique des rapports de force et la protection contre les dommages qui naissent dans le cyberspace (en posant des limites efficacement appliquées aux pratiques et aux comportements en ligne, le cas échéant en se servant de prescriptions numériques pour renforcer cette efficacité d'application) ; la conservation ou le développement de compétences juridiques propres à l'État, qui bénéficient à la population et qui ne sont pas ou qui sont mal exercées par les acteurs privés sur internet.

Le cyberspace est donc encore un lieu d'affrontement intense entre la souveraineté étatique et les actions des acteurs privés, très amplifiées par le mode prescriptif numérique en ligne. Nos travaux nous font toutefois conclure qu'il est inexact de considérer le cyberspace comme étant techniquement insusceptible d'être étatisé. La structure maillée et mondialement interconnectée du réseau internet ne font pas obstacle à son étatisation. L'État peut lui-même être un prescripteur numérique central : d'un point de vue technique, rien ne l'empêche d'être opérateur de transmission (ex-France Telecom par exemple), administrateur d'applications (service-public.fr, France Connect, Parcoursup...), gestionnaire de serveurs (Afnic qui gère les serveurs DNS des <.fr>, <.paris>, <.ovh>...), fabricant de machines numériques, utilisateur et programmeur (à travers ses agents publics ou des personnes privées rémunérées par l'État). Rien n'empêche l'État de centraliser son réseau internet de telle manière qu'il soit quasiment inaccessible depuis l'étranger, et qu'il n'autorise quasiment aucune sortie de données vers l'étranger (Corée du Nord et, dans une moindre mesure, Chine). Rien n'empêche chaque État de créer son « propre » réseau internet à la manière

de la Corée du Nord, de créer son propre réseau DNS à l'image de la Russie, de contrôler la gestion et l'administration des applications comme le fait la Chine à travers les équipes de modération des applications.

L'étatisation d'internet est possible techniquement, mais elle est rarement efficace. Premièrement, un État qui isole son réseau internet de l'internet mondial se prive d'un volume considérable de ressources financières faute d'échanges économiques avec l'étranger sur internet. Un internet étatique isolé peut appauvrir l'État et, faute d'économie numérique en ligne, le rendre paradoxalement très dépendant des ressources étrangères (économiques et informatiques) pour préserver son isolement. C'est par exemple le cas de la Corée du Nord, totalement dépendante de la Chine pour la fabrication de ses propres smartphones, et doublement dépendante de la Chine et de la Russie pour se connecter au réseau internet mondial (l'AS nord-coréen étant seulement connecté à un AS russe et à un AS chinois). Deuxièmement, un État qui centralise excessivement son réseau le rend très vulnérable à la diffusion rapide d'un logiciel malveillant sur le réseau. On l'a vu en Corée du Nord, où une seule cyberattaque a fait s'effondrer l'ensemble du réseau internet national. On l'a aussi observé en Russie, où la centralisation du réseau DNS fragilise l'ensemble de l'internet russe en cas d'erreur humaine ou de cyberattaque.

Troisièmement, un État qui joue excessivement le rôle de prescripteur numérique sur internet - en nationalisant ou en contrôlant les opérateurs, les fabricants, la gestion des serveurs voire les applications - engage des coûts très importants et se prive des avantages qu'offre la concurrence privée pour la satisfaction de la demande. Or, les coûts engagés ne s'accompagnent pas d'une baisse du risque de contournement : on l'a constaté en Chine où les contournements massifs sont fréquents malgré un contrôle étatique particulièrement vaste sur les prescripteurs numériques les plus centraux dans le pays. De même, une nationalisation excessive peut frustrer la demande à défaut de concurrence privée, ce qui peut conduire les prescripteurs à délaisser l'offre proposée par l'État et à contourner les restrictions étatiques pour accéder à des offres illicites : on l'a remarqué en Corée du Nord, avec les contournements massifs de la population nord-coréenne pour consommer des biens culturels étrangers dématérialisés, faute d'une offre nationale satisfaisante en la matière.

En somme, on en conclut que la régulation nord-coréenne d'internet est très inefficace pour préserver la souveraineté numérique du pays, à la fois très dépendante de la Chine et de la Russie, soumise à un réseau national très vulnérable, et en proie à des contournements massifs de la population qui accède à des contenus de nature à mettre en péril la légitimité de l'État nord-coréen. On a aussi beaucoup expérimenté la souveraineté numérique de la Russie, très dépendante d'entreprises étrangères jugées ennemies de la Nation (notamment Meta), échouant à faire adopter par sa population ses applications nationales promues par la Fédération (Rutube, YAPPY, Rosgram...), échouant à pratiquer le filtrage à l'échelle fédérale, et aggravant la vulnérabilité de son réseau internet national à travers son réseau DNS.

De ces trois pays, seule l'étatisation chinoise nous semble assez efficace par son équilibre entre centralisation de la gestion du réseau et décentralisation de son fonctionnement, entre restrictions des services étrangers et promotion des services nationaux, entre échanges économiques étrangers et flux économiques nationaux. Cependant, la Chine reste elle aussi soumise à des contournements de très grande ampleur par sa population pour échapper à la censure, et l'inefficacité de la régulation en la matière ne doit pas être minimisée sur le territoire

chinois. Chaque pays a ses propres objectifs de régulation en fonction des intérêts qu'il cherche à préserver. En Chine, le maintien du lien de confiance entre la population et le gouvernement est un objectif fondamental. La divulgation d'affaires d'État (train qui déraile, gestion de la pandémie de Covid19, Peng Shuai, traite des êtres humains dissimulée par l'État...) est un problème grave et récurrent sur l'internet chinois, et l'échelle de diffusion acquise par ces divulgations rend compte de l'inefficacité de la régulation chinoise dans ce domaine.

Côté occidental, les réseaux français et britanniques sont suffisamment décentralisés pour ne pas souffrir des mêmes vulnérabilités que la Corée du Nord et la Russie. Cependant, ces pays restent technologiquement très dépendants, principalement des fabricants américains, sud-coréens et chinois voire japonais, ainsi que des administrateurs d'applications et des gestionnaires de serveurs américains voire, de plus en plus, chinois (TikTok, Alibaba, Aliexpress, Temu, Shein...). Les dépendances de la France et du Royaume-Uni sont de plus en plus diversifiées, limitant le risque d'une dépendance à un seul ou à un petit nombre de pays et d'acteurs privés. Les pays européens sont toutefois encore loin d'égaler l'indépendance technologique chinoise.

On n'observe pas d'efficacité supérieure ni inférieure des techniques de restriction françaises et britanniques par rapport à celles chinoises : la France, le Royaume-Uni et la Chine semblent souffrir d'un contournement à peu près équivalent. Toutefois, la divulgation des affaires d'État nous semble moins problématique en France et au Royaume-Uni, car ces deux États n'en font pas une priorité à travers leurs normes juridiques contrairement à la Chine. Les objectifs de régulation en France et au Royaume-Uni sont différents par rapport à la Chine. Conformément à leur légitimité libérale, la France et le Royaume-Uni visent en priorité la lutte contre les dommages infligés aux individus plutôt qu'à l'État, visent le respect des droits et libertés de chacun plutôt que la confiance entre la population et l'État. La vaste diffusion de contenus haineux, de cyberharcèlement, de consommation illicite d'oeuvres protégées ou encore d'arnaques en ligne sur les réseaux britannique et français rendent compte de l'inefficacité de la régulation française et britannique sur ces objectifs libéraux de régulation.

En somme, quelle conclusion tire-t-on de l'efficacité de la régulation dans chacun de ces ordres juridiques par rapport à leur souveraineté numérique et par rapport à leurs propres objectifs de régulation ? On rappelle avoir défini la souveraineté numérique des États comme une doctrine recherchant l'application des principes de souveraineté étatique aux technologies numériques, à savoir : la compétence des États (donc leur autorité) pour encadrer les technologies qui affectent leur population, leur territoire ou leurs administrations ; l'exclusivité de la compétence sur le territoire national et la plénitude des compétences internationales ; et l'indépendance des États et de leur population vis-à-vis des puissances technologiques privées et/ou étrangères. Parmi les États étudiés, seule la Chine parvient à réguler efficacement internet par rapport à sa souveraineté numérique, tandis que la France et le Royaume-Uni sont assez peu efficaces, et que la Russie et la Corée du Nord sont peu voire très peu efficaces. Quant à leurs propres objectifs de régulation (politique d'isolement à l'égard des informations étrangères en Corée du Nord, préservation des libertés et droits individuels au Royaume-Uni et en France, lutte contre la divulgation des affaires d'État en Chine...), aucun des États étudiés ne parvient à adopter une régulation efficace d'internet pour atteindre ces objectifs si l'on s'en tient à l'échelle de diffusion acquise sur ces réseaux par des données illicites ou refusées par le régulateur.

4/ Efficacité du contrôle de l'échelle de diffusion d'une donnée par des normes juridiques

On a distingué deux types de données par rapport au régulateur : les données refusées par le régulateur (R-DATA), telles les données illicites ; et les données admises par le régulateur (A-DATA), telles les données licites. On a constaté que l'échelle de diffusion d'une donnée dans le cyberspace peut résulter de quatre forces (quatre causes) dont les effets se contredisent : l'attachement du prescripteur à produire ou à stocker une donnée ; son détachement à la produire ou à la stocker ; l'aléa avec lequel il la produit ou la stocke ; et l'incident qui le conduit à la produire ou à la stocker.

On a démontré qu'il est possible de réguler ces rapports de force pour contrôler l'échelle de diffusion d'une R-DATA. Dans ce cadre, on a ensuite identifié quatre hypothèses pour réduire l'échelle de diffusion d'une R-DATA :

- Si l'échelle de diffusion d'une R-DATA est majoritairement intentionnelle, et constituée par un degré élevé d'attachement, on invite le régulateur à *prioriser* l'essor de « données de substitution », c'est-à-dire des A-DATA chargées de concurrencer cette R-DATA, tout en favorisant la restriction de l'accès à cette R-DATA ;
- Si l'échelle de diffusion d'une R-DATA est majoritairement intentionnelle, et constituée par un faible degré d'attachement, on invite le régulateur à *prioriser* des restrictions dissuasives pour l'accès à cette R-DATA, mais aussi à favoriser l'essor de données de substitution ;
- Si l'échelle de diffusion d'une R-DATA est majoritairement accidentelle, et constituée par un degré élevé d'aléa, on invite le régulateur à *prioriser* l'essor de « moyens de contrôle » intensifs, c'est-à-dire des techniques de restriction mises à la disposition des prescripteurs numériques pour empêcher la production ou le stockage de cette R-DATA ;
- Si l'échelle de diffusion d'une R-DATA est majoritairement accidentelle, et constituée par un faible degré d'aléa, on invite le régulateur à prioriser l'essor de moyens de contrôle.

On en conclut que les normes juridiques peuvent permettre de contrôler l'échelle de diffusion d'une R-DATA dans le cyberspace en satisfaisant la demande (grâce à des techniques d'augmentation) et en octroyant aux utilisateurs des moyens de se défendre contre le stockage de données indésirables (grâce à des techniques de restriction contrôlées par les prescripteurs). Cependant, ces techniques ne peuvent pas être mises en œuvre dans n'importe quelles conditions.

D'une part, les données de substitution ne peuvent être efficaces que si elles offrent plus d'avantages aux prescripteurs que ne le fait la R-DATA substituée (valeur ajoutée de la donnée de substitution) et/ou si elles bénéficient d'un volume de prescripteurs qui y accèdent supérieur au volume dont bénéficie la R-DATA (effet de réseau profitant à la donnée de substitution). On a vu que, pour offrir de meilleurs avantages aux prescripteurs, la donnée de substitution nécessite d'importants efforts (investissement en R&D et recherche fondamentale, donnée de substitution à la fois novatrice et fédératrice, ou poussée par des circonstances exceptionnelles, ouverture du marché des données de substitution, organisation structurée de programmations/planifications...). On a vu aussi qu'il existe plusieurs moyens pour conforter l'effet de réseau profitant à une donnée de substitution (surexposition de la donnée de substitution, réutilisabilité de la donnée de substitution, accélération discriminée

ou redirection du trafic vers la donnée de substitution, insertion de la donnée de substitution avec d'autres données déjà très utilisées...). D'autre part, les moyens de contrôle ne peuvent à leur tour être efficaces que s'ils couvrent les lacunes de contrôle qui conduisent les prescripteurs à stocker accidentellement la R-DATA.

Par ailleurs, on a démontré que la régulation de l'échelle de diffusion d'une donnée ne peut qu'être cyclique, en s'adaptant constamment à l'évolution technique sur internet, à l'évolution des R-DATA et à l'évolution de l'équilibre Attachement/Détachement/Incident/Aléa qui caractérise une échelle de diffusion. Enfin, on a souligné que, pour être efficace, une technique de régulation mise en œuvre à l'égard d'une R-DATA ou A-DATA ne doit pas dépasser le périmètre de cette R-DATA ou A-DATA.

5/ Quels prescripteurs en ligne sont les plus puissants pour contrôler l'échelle de diffusion d'une donnée dans le cyberspace ?

Nos travaux en arrivent à la conclusion qu'il n'existe pas une catégorie de prescripteurs numériques qui serait statutairement plus puissante que les autres pour contrôler une échelle de diffusion. Tout dépend de la R-DATA ou de la A-DATA concernée, et de la constitution de son échelle de diffusion.

D'une part, la puissance d'une catégorie de prescripteurs numériques sur l'échelle de diffusion d'une donnée dépend de la R-DATA/A-DATA impliquée. Par exemple, l'échelle de diffusion de la R-DATA « transmission de logiciels malveillants sur le réseau public » est très largement – voire quasi exclusivement – alimentée par les opérateurs de transmission. Ils sont les prescripteurs qui possèdent le plus de pouvoir sur cette échelle de diffusion. Cela ne signifie pas nécessairement qu'ils ont les moyens de réduire effectivement cette échelle de diffusion, mais qu'ils sont ceux qui peuvent le plus réduire ladite échelle car ils en représentent la part la plus importante. Inversement, l'échelle de diffusion de la R-DATA « téléchargement de logiciels malveillants » est majoritairement alimentée par les utilisateurs. Ils sont alors les acteurs les plus puissants pour réduire cette échelle de diffusion, car ils en représentent la plus grande part. Là encore, cela ne signifie pas qu'ils ont les moyens d'exercer leur pouvoir.

D'autre part, la puissance effective d'une catégorie de prescripteurs numériques sur l'échelle de diffusion d'une R-DATA/A-DATA dépend de la constitution de cette échelle. Pour reprendre l'exemple des R-DATA « transmission de logiciels malveillants sur le réseau public » et « téléchargement de logiciels malveillants », l'échelle de diffusion de ces données est très majoritairement accidentelle. Les opérateurs de transmission et les utilisateurs doivent donc bénéficier de moyens de contrôle pour exercer leur puissance sur l'échelle de diffusion de ces R-DATA et empêcher leur stockage accidentel. Ces moyens de contrôle peuvent être mis à leur disposition par d'autres prescripteurs numériques, ou encore par des institutions externes au cyberspace (telle l'Autorité nationale de sécurité des systèmes d'information en France) : pour réduire l'échelle de diffusion de la R-DATA « transmission de logiciels malveillants sur le réseau public », les programmeurs peuvent fournir aux opérateurs des logiciels de détection des malwares et l'Anssi peut leur fournir des conseils de sécurisation du réseau ; de même, pour réduire l'échelle de diffusion de la R-DATA « téléchargement de logiciels malveillants », les opérateurs peuvent mettre à disposition des utilisateurs des solutions antivirus, et des outils pour gérer les flux entrants de données. **Les prescripteurs les plus « puissants » sur une échelle de diffusion nécessitent donc bien souvent l'aide d'autrui pour exercer leur puissance effective.** Cette conclusion se vérifie aussi bien pour les R-DATA intentionnelles, telle que la

consommation illicite de biens culturels : les utilisateurs sont certes les prescripteurs les plus puissants pour contrôler l'échelle de diffusion de cette R-DATA, car ils sont ceux qui en représentent la plus grande part ; mais des données de substitution (offre légale) doivent être mises à leur disposition pour que soit effectivement réduite cette échelle.

Contrairement à la théorie *Code Is Law* qui mise sur les programmeurs, on n'identifie donc pas une catégorie de prescripteurs qui serait statutairement et systématiquement plus puissante que les autres pour maîtriser ce qui est diffusé dans le cyberspace. Tout dépend de la R-DATA/A-DATA impliquée, de la constitution de son échelle de diffusion, et de l'aide apportée par les autres acteurs aux prescripteurs qui contribuent le plus à une échelle de diffusion. On l'explique par le fait que le processeur ne hiérarchise pas les données à exécuter selon la catégorie humaine qui les exécute (mais selon la priorité de la requête dans le cadre d'une interruption/exception, et selon le niveau de privilège mémoire auquel appartient une donnée). En ce sens, on a démontré : que l'exercice par l'utilisateur de son pouvoir de contrainte sur la machine pour produire une donnée peut entraîner une échelle de diffusion supérieure à l'échelle acquise par les données issues d'un programmeur ; et que les programmeurs n'ont qu'une très faible maîtrise sur les usages que font les utilisateurs de leurs programmes. Le fait que les capacités d'action des utilisateurs soient fondées sur les règles programmées ne se traduit donc pas par une supériorité du programmeur sur l'utilisateur en termes de pouvoir dans les rapports de force interhumains en ligne. La puissance d'un prescripteur sur l'échelle de diffusion d'une donnée dans le cyberspace est relative, et varie selon les circonstances déjà décrites.

6/ Les limites de la méthodologie

La méthodologie employée dans le cadre de cette thèse s'accompagne de plusieurs limites qui doivent conduire à ne pas généraliser nos conclusions sur la régulation des rapports de force interhumains en ligne. On identifie trois limites principales.

La première, la plus importante, concerne le regard endogène que l'on porte sur internet pour comprendre et réguler les rapports de force interhumains qui se jouent dans le cyberspace. Certes, dès lors qu'on a défini le cyberspace comme l'ensemble des mémoires informatiques connectées à internet, seule une méthodologie endogène peut permettre de comprendre les rapports de force qui résultent du cyberspace. Cependant, tous les rapports de force interhumains qui ont internet pour objet ne naissent pas du cyberspace lui-même. On l'a souligné en Introduction : un employé fraîchement licencié qui, par vengeance, détruit les machines connectées à internet de son entreprise s'inscrit dans un rapport de force qui a internet pour objet, mais ce rapport de force naît d'une source externe à la machine et non d'une production de données stockées par la machine. De même, les rapports de force économiques qui ont internet pour objet ne naissent pas non plus du cyberspace, *i.e.* du stockage et de l'exécution de données binaires. Ou encore les rapports de force géopolitiques qui se jouent sur les câbles sous-marins ne proviennent pas non plus du cyberspace. Les études exogènes nous semblent donc nécessaires pour compléter notre travail et cerner ces rapports de force interhumains sur internet qu'on n'a pas ou qu'on a peu analysés. Aussi importe-t-il de comprendre que nos conclusions ne s'appliquent qu'aux rapports de force interhumains nés du cyberspace (qu'on a baptisés « rapports de force interhumains en ligne »), et non à tous les rapports de force interhumains qui ont internet pour objet.

Cette conception endogène nous a aussi conduit à circonscrire notre champ d'étude à l'efficacité des seules techniques de régulation internes au réseau (suppression de données,

chiffrement, blocage, filtrage, surexposition...), et non à celles qui lui sont extérieures (amendes, peines de prison, dommages-intérêts, retraits de licences, négociations avec les acteurs économiques, immatriculation des drones connectés et structures militaires de détection des drones ennemis...). Or, il est tout à fait probable que les techniques de régulation externes à internet jouent un rôle déterminant pour réduire l'échelle de diffusion d'une donnée en ligne - telle une peine de prison qui dissuaderait quiconque de produire une R-DATA. À nouveau, les études exogènes nous semblent donc indispensables pour évaluer l'efficacité des techniques de régulation externes sur l'échelle de diffusion d'une donnée.

En plus de ce regard endogène, la deuxième limite qu'on reconnaît à notre méthodologie réside dans notre étude circonscrite à la régulation de l'échelle de diffusion d'une donnée. En effet, on a vu que les rapports de force interhumains en ligne (*i.e.* issus du cyberspace) peuvent jouer sur l'échelle de diffusion d'une donnée ou sur l'importance critique de la machine qui stocke cette donnée. Par exemple, une cyberattaque dirigée contre les terminaux d'un hôpital aura certes une échelle de diffusion moindre par rapport à une cyberattaque dirigée contre 5 000 terminaux de particuliers ; mais l'attaque dirigée contre l'hôpital aura de plus grave répercussions en raison de l'importance critique de la structure hospitalière. Cela signifie que notre théorie de la régulation ne propose pas de réguler la gravité des dommages nés du cyberspace, mais seulement l'échelle de diffusion des dommages nés du cyberspace. Par conséquent, la régulation ici proposée ne couvre pas complètement les rapports de force interhumains nés du cyberspace, et demande à être complétée par une théorie de la régulation de ces rapports de force élaborée sur la base de la gravité des dommages en ligne.

Enfin, la troisième limite principale de notre méthodologie réside dans le pari théorique de la régulation. Tout problème peut-il être résolu par régulation ? Cette thèse soutient que l'échelle de diffusion d'une donnée peut être contrôlée en jouant sur l'équilibre Attachement/Détachement/Incident/Aléa qui compose une échelle de diffusion. Cependant, en l'absence d'expérimentation à grande échelle et à long terme, cette proposition reste à l'état théorique. Rappelons d'ailleurs que les techniques de régulation externes au cyberspace peuvent avoir un effet sur l'échelle de diffusion et sur la gravité des dommages nés du cyberspace (par exemple, l'éducation de la population à des connaissances en cybersécurité pour se préserver des logiciels malveillants et ainsi limiter leur échelle diffusion). Aussi, et bien que cette thèse se soit spécialisée dans la régulation technique des rapports de force interhumains en ligne, on invite le régulateur à se garder de tout technocentrisme. La technologie n'est pas la solution à tous les problèmes, y compris aux problèmes technologiques.

La théorie qu'on propose nous semble valable pour tout réseau numérique qui partage les caractéristiques d'internet, quel que soit l'objectif du régulateur, quelle que soit la culture de la population concernée par la régulation. À notre connaissance, l'intelligence artificielle de remet pas en cause le fait que les données aient la nature de « prescriptions numériques », ni même leurs conditions de production (ouvertes et égalitaires), d'exécution (neutres et aliénées par interopérabilité) et d'ordonnancement (ubiquitaires et diffusibles) identifiées dans cette thèse. Elle ne remet pas davantage en cause le fait que les prescripteurs peuvent soit cesser, soit persister d'accéder à une donnée une fois restreint l'accès à cette donnée, pas plus qu'elle ne met en doute le fait que les êtres humains contribuent à l'échelle de diffusion d'une donnée en y accédant soit intentionnellement, soit accidentellement.

L'IA va très probablement bouleverser notre réalité sociale, économique et technologique voire institutionnelle sur de très nombreux aspects, mais les progrès faits ces dernières années

ne nous semblent pas contredire la grille de lecture proposée dans cette thèse pour contrôler l'échelle de diffusion d'une donnée. En revanche, on peut s'attendre à une hausse du nombre d'accès accidentels à des R-DATA, car on a vu que l'être humain ne peut pas avoir le plein contrôle sur les décisions de l'IA, autonome dans ses apprentissages. On peut s'attendre à un cyberspace plus chaotique, dans lequel les virus informatiques intelligents s'adaptent aux failles de la machine affectée, dans lequel des antivirus intelligents s'adapteront à leur tour, sans que l'être humain ait de rôle central dans ces rapports de force entre IA. On peut s'attendre à un cyberspace moins « contrôlable » qu'avant, non à cause des comportements des prescripteurs humains, mais de ceux de l'IA. Il faudra alors rechercher comment réguler les rapports de force inter-IA en ligne.

Table des matières

REMERCIEMENTS.....	1
SOMMAIRE	2
INTRODUCTION	3
PREMIÈRE PARTIE – L'ÉTUDE DES RAPPORTS DE FORCE INTERHUMAINS EN LIGNE	24
Sous-Partie 1. L'identification des rapports de force en ligne par les États et chercheurs.....	25
Chapitre 1. La conception exogène du réseau internet.....	26
Section 1. La distanciation du réseau et de ses acteurs par la machine selon l'axe hardwariste....	26
Paragraphe 1. Le fonctionnement du réseau internet.....	26
A) <i>Le réseau électrique en toute technicité.....</i>	26
B) <i>Le réseau numérique, créateur d'une nouvelle réalité.....</i>	29
C) <i>Internet, réseau prodige.....</i>	33
Paragraphe 2 - L'analyse hardwariste des rapports de force en ligne.....	38
Section 2. La distanciation du réseau et de ses acteurs par leur humanité selon l'axe social	45
Paragraphe 1 - La lecture pragmatique des rapports de force en ligne	45
A) <i>Enjeux pratiques des fournisseurs de services en ligne</i>	45
B) <i>Enjeux pratiques des acteurs institutionnels publics et privés d'internet.....</i>	49
Paragraphe 2 - La lecture informationnelle des rapports de force en ligne	53
A) <i>La donnée-information saisie matériellement par l'être humain.....</i>	53
B) <i>La donnée-information saisie immatériellement par l'être humain</i>	57
Chapitre 2. La conception endogène du réseau internet	62
Section 1. Une normativité issue d'un « cyberspace »	62
Paragraphe 1 - L'absorption de l'être humain dans une normativité machinale.....	62
A) <i>L'autonomie de la Machine</i>	62
B) <i>La fusion normative de l'Homme et de la Machine</i>	66
Paragraphe 2 - La vie normative du cyberspace	70
A) <i>L'autarcie normative du réseau.....</i>	70
B) <i>Le jeu normatif par le langage informatique : Code is Law</i>	73
Section 2. Normativités croisées au sein du cyberspace	78
Paragraphe 1 - Un éparpillement de foyers normatifs scientifiquement articulés	78
A) <i>Une normativité communicationnelle en ligne.....</i>	78
B) <i>Autres normativités identifiées en ligne</i>	85
Paragraphe 2 - Le croisement de foyers normatifs juridiquement régulés	90
A) <i>De nouveaux rôles normatifs reconnus aux acteurs d'internet</i>	90
B) <i>De nouveaux pouvoirs normatifs reconnus aux acteurs d'internet</i>	95
Sous-Partie 2. La clandestinité (scientifico-étatique) des prescriptions numériques.....	103
Chapitre 1. Le caractère prescriptif des données numériques.....	103
Section 1. Le choix d'une méthodologie endogène pour l'étude des rapports de force en ligne .	104
Paragraphe 1 – Des rapports de force inexplicables par l'investigation endogène d'internet.....	104
A) <i>L'insuffisance des études endogènes pour la compréhension du pouvoir de l'internaute.....</i>	104
B) <i>Des explications exogènes au secours des insuffisances endogènes.....</i>	108
Paragraphe 2 – La pertinence du regard interne pour la compréhension de mouvements externes .	111
A) <i>Lois internes et lois externes d'un objet.....</i>	111
B) <i>Lois internes et environnement externe de l'objet.....</i>	114
Section 2. Les prescriptions numériques.....	117
Paragraphe 1 – L'action prescriptive de la donnée binaire.....	118
A) <i>La compréhension machinale de l'action binaire.....</i>	118
1. La production, la mémorisation (le « stockage ») et l'exécution des données.....	118
2. Les données d'instruction	122
B) <i>Le mode d'action prescriptif de l'ordre binaire</i>	125
Paragraphe 2 – Comparaison des processus prescriptifs juridico-étatique et numérique	128
A) <i>Modélisation simple du processus prescriptif juridico-étatique</i>	129
B) <i>Modélisation simple du processus prescriptif numérique</i>	137
Chapitre 2. Le mode prescriptif numérique des données en ligne.....	145

Section 1. Comparaison des relations inter-prescriptives étatiques et numériques	145
Paragraphe 1 – Modélisation complexe du processus prescriptif étatique	145
Paragraphe 2 – Comparaison avec la modélisation complexe du processus prescriptif numérique	155
Section 2. Prescriptions numériques internes et rapports de force interhumains externes	165
Paragraphe 1 - Les lois internes à l'activité numérique	165
A) <i>Lois internes imputables à la structure numérique locale d'une machine-hôte (« lois internes locales »)</i>	165
B) <i>Lois internes imputables à la structure numérique en réseau de machines connectées (« lois internes au réseau »)</i>	168
Paragraphe 2 – L'influence des lois numériques internes sur les rapports de force interhumains	171
A) <i>Mode prescriptif numérique et pouvoir de prescrire en ligne</i>	171
B) <i>Mode prescriptif numérique et rapports de force interhumains en ligne</i>	176
Section 3. Les leçons des échecs de l'explication Code Is Law	182
Paragraphe 1. L'effondrement de l'explication Code is Law	183
A) <i>Le code binaire, cause de la contrainte machinale</i>	183
B) <i>Les différents prescripteurs numériques</i>	186
Paragraphe 2. Le cyberspace, à la fois bien commun de fait et réalité prescriptive	189
 DEUXIÈME PARTIE – LA RÉGULATION DES RAPPORTS DE FORCE INTERHUMAINS EN LIGNE	 195
Sous-Partie 1. Techniques basiques de restriction de l'accès à internet	195
Chapitre 1. Introduction à la régulation d'internet	196
Section 1. La régulation juridico-étatique d'internet	196
Paragraphe 1 – Les bases du concept de régulation juridique	196
A) <i>Introduction au concept de régulation</i>	196
1. <i>Histoire scientifique de la régulation</i>	196
2. <i>Définition proposée de la régulation</i>	203
B) <i>Les antécédents de la régulation juridique en France</i>	206
Paragraphe 2 – La régulation juridique d'internet	210
A) <i>La consécration de la régulation juridique en France</i>	210
1. <i>L'essor de la régulation juridique dans les années 1970-1980 en France</i>	210
2. <i>La France des années 2020, submergée par la régulation juridique</i>	215
B) <i>Concepts mobilisés pour réguler juridiquement le réseau internet</i>	221
Section 2. Les types de restriction d'accès selon la source de la restriction	226
Paragraphe 1 – La restriction de la transmission de données	226
A) <i>La coupure de la transmission</i>	227
B) <i>Le ralentissement de la transmission</i>	234
Paragraphe 2 – La restriction du stockage de données	236
A) <i>Introduction à la restriction du stockage de données : les exemples du chiffrement et de l'avertissement</i>	236
1. <i>Le hachage, technique basique du chiffrement</i>	236
2. <i>La signature électronique, technique authenticatrice du chiffrement</i>	239
3. <i>L'avertissement</i>	246
B) <i>La suppression de données</i>	248
1. <i>Les types de données supprimables : les exemples des comptes utilisateurs, des contenus et des fonctions logicielles</i>	248
2. <i>Méthode de suppression de données : l'exemple du déréférencement</i>	254
Chapitre 2. Les techniques de blocage et de filtrage de l'accès	260
Section 1. La technique du blocage	261
Paragraphe 1 – Le blocage de la transmission et du stockage de données	261
A) <i>Le blocage dès la transmission</i>	261
1. <i>Le blocage dès l'acheminement en Chine et en Russie</i>	261
2. <i>Le blocage dès l'acheminement en France, au Royaume-Uni et aux États-Unis</i>	265
B) <i>Le blocage du stockage de données : l'exemple du bannissement total par blocage</i>	269
C) <i>Le blocage du stockage de données : l'exemple du bannissement partiel par blocage</i>	273
Paragraphe 2 – Le blocage du stockage de contenus et de logiciels tiers	277
A) <i>Le masquage de contenus</i>	277
B) <i>Le blocage par non-interopérabilité</i>	282
Paragraphe 3 – La désactivation de fonctions logicielles par blocage	284
A) <i>Étude de cas : l'efficacité du blocage de fonctions par TikTok en Russie</i>	284

1.	Présentation de la technique de désactivation de fonctions par blocage	284
2.	L'efficacité de la régulation de TikTok en Russie pour empêcher l'accès aux informations étrangères et l'opposition au gouvernement	288
B)	<i>Efficacité de la restriction russe à l'aune de la souveraineté numérique</i>	292
1.	La doctrine de la souveraineté numérique	292
2.	Évaluation de l'efficacité des restrictions en Russie pour le développement de sa souveraineté numérique	301
Section 2. La technique du filtrage		306
Paragraphe 1 – Le filtrage de la transmission de données		306
A)	<i>Le filtrage en ligne dès l'acheminement</i>	306
B)	<i>Le filtrage local dès l'acheminement</i>	312
Paragraphe 2 – Le filtrage du stockage de données		318
A)	<i>Techniques de filtrage local</i>	319
B)	<i>Techniques de filtrage en ligne : comparaison des filtres manuel et automatisé</i>	324
C)	<i>Le filtrage de contenus dès les serveurs</i>	332
Sous-Partie 2. Étude de l'efficacité régulatrice sur internet		336
Chapitre 1. La technique de la centralisation du réseau		337
Section 1. La centralisation de la transmission de données et des noms de domaine		337
Paragraphe 1 – La centralisation de la transmission de données		337
A)	<i>La centralisation du transport sous-marin</i>	337
B)	<i>La centralisation de l'acheminement : métriques de la centralisation</i>	348
C)	<i>La centralisation de l'acheminement : comparaisons internationales</i>	355
1.	Comparaison des réseaux nationaux d'acheminement	355
2.	Conclusions sur la centralisation des réseaux nationaux d'acheminement	360
D)	<i>L'internet le plus centralisé au monde : le cas de la Corée du Nord</i>	366
1.	La connexion du réseau IP	366
2.	La centralisation étatique nord-coréenne du réseau IP	369
Paragraphe 2 – La centralisation du stockage de données : l'exemple des noms de domaine		377
A)	<i>Centralisation et décentralisation du réseau DNS</i>	377
B)	<i>Naissance d'un National DNS (NDNS) : la centralisation russe de l'accès aux noms de domaine</i>	384
Section 2. La centralisation dès le stockage des usages en ligne		391
Paragraphe 1 – La centralité de connexion des applications		391
A)	<i>Évaluation de la centralité d'une application</i>	391
B)	<i>Les bonds exceptionnels des applications fédératrices et novatrices</i>	396
C)	<i>Les bonds exceptionnels des applications du fait de leur insertion ou de circonstances extraordinaires</i>	402
Paragraphe 2. Les centralités de gestion et de fonctionnement des applications en ligne		410
A)	<i>L'aggravation de la centralité de connexion par la centralité de gestion</i>	410
1.	L'appropriation des principaux segments de marché par les géants	410
2.	Conclusion sur la centralisation de gestion des applications en ligne entre 2008 et 2022	416
B)	<i>La centralité de fonctionnement des applications en ligne</i>	421
Chapitre 2. Évaluation de l'efficacité de l'action régulatrice sur internet		430
Section 1. Techniques de régulation par augmentation de l'accès		430
Paragraphe 1 – Techniques pour augmenter incidemment l'accès à des A-DATA		430
A)	<i>La décentralisation de l'accès à internet</i>	430
B)	<i>Le raccordement de l'accès à internet</i>	435
1.	Les politiques de raccordement au Royaume-Uni	435
2.	Les politiques de raccordement en France	439
C)	<i>L'accélération non-discriminée de l'accès à internet</i>	442
Paragraphe 2 – Techniques basées sur le trafic pour augmenter spécifiquement l'accès aux A-DATA		450
A)	<i>L'accélération discriminée de l'accès à une A-DATA dès la transmission de données</i>	450
B)	<i>La redirection de l'accès vers une A-DATA depuis l'acheminement de données</i>	454
1.	Avantages de la redirection vers une A-DATA	454
2.	Inconvénients de la redirection vers une A-DATA	460
C)	<i>La redirection de l'accès vers une A-DATA depuis le stockage de données</i>	463
Paragraphe 3 – Techniques basées sur les services et les contenus pour augmenter spécifiquement l'accès à une A-DATA		467

A) <i>La création et/ou la pluralisation des services admis par le régulateur : l'exemple de la Chine</i>	468
1. La stratégie technologique chinoise	468
2. Le plan Made in China 2025	472
B) <i>La pluralisation des contenus admis par le régulateur</i>	477
C) <i>Avantages et inconvénients de la pluralisation de A-DATA</i>	479
1. Premier avantage de la pluralisation de A-DATA : l'augmentation des capacités des utilisateurs à consommer légalement	479
2. Deuxième avantage de la pluralisation de A-DATA : la réduction du risque de contournement	485
3. Inconvénients de la pluralisation de A-DATA	487
D) <i>La surexposition et la réutilisabilité d'une A-DATA</i>	490
1. La surexposition d'une A-DATA	490
2. La réutilisabilité d'une A-DATA	498
Section 2. Théorisation de l'efficacité de la régulation du cyberspace	503
Paragraphe 1 – Les configurations de contournement	503
A) <i>Les configurations de contournement qui ne reposent pas sur des intermédiaires</i>	504
1. La migration	504
2. La feinte	509
B) <i>Les configurations de contournement qui reposent sur des intermédiaires</i>	515
1. Le saut	515
2. L'affranchissement	520
C) <i>Les configurations de contournement qui reposent sur des périphériques accessoires</i>	524
Paragraphe 2. Le contrôle de l'échelle de diffusion d'une donnée sur internet	529
A) <i>Les équilibres de régulation de l'échelle de diffusion d'une donnée en ligne</i>	529
1. Les motivations des prescripteurs à produire ou stocker des données en ligne	529
2. Le fonctionnement des équilibres de régulation de l'échelle de diffusion d'une donnée en ligne	532
B) <i>Propositions théoriques pour contrôler l'échelle de diffusion d'une donnée en ligne</i>	537
1. Moyens de contrôle et données de substitution	537
2. Les cycles de régulation	543
CONCLUSION	547

Bibliographie indicative

Théorie du droit

1. Ouvrages scientifiques

- ALEXY Roberts, *A Theory of Constitutional Rights*, Oxford University Press, 2002
[publication originale en allemand en 1986], p. 47-50
- BARRAUD Boris, *Repenser la pyramide des normes à l'ère des réseaux. Pour une conception pragmatique du droit*, L'Harmattan, 2012
- BARRAUD Boris, *Le droit postmoderne. Une introduction*, L'Harmattan, 2017
- CARBONNIER Jean, *Sociologie juridique*, Quadrige Manuels, 2016
- CARRÉ DE MALBERG René, *Contribution à la Théorie générale de l'État*, Dalloz, 2004
- GUASTINI Riccardo, *Leçons de théorie constitutionnelle*, préc., Dalloz, 2010
- KELSEN Hans, *Théorie pure du droit*, 2^e édition, Paris, PUF, 1996
- LUHMANN Niklas, *Grundrechte als Institution. Ein Beitrag zur politischen Soziologie*, Dunker & Humblot, 2009
- OST François et VAN DE KERCHOVE Michel, *De la pyramide au réseau ?*, Bruxelles, F.U.S.L., 2002
- PAPATOLIAS Apostolos, *Conception mécaniste et conception normative de la constitution*, Thèse en droit public, Sakkoulas, 2000
- POSNER Richard, *Pragmatism, Law and Democracy*, Harvard University Press, 2003
- ROBÉ J.-P., LYON-CAEN Antoine et VERNAC Stéphane (dir.), *Multinationals and the Constitutionalization of the World Power System*, Routledge, 2016
- TEUBNER Gunther, *Fragments constitutionnels. Le constitutionnalisme sociétal à l'ère de la globalisation*, Classiques Garnier, 2016
- TROPER Michel, CHAMPEIL-DESPLATS Véronique et GRZEGORCZYK Christoph (dir.), *Théorie des contraintes juridiques*, LGDJ, Bruylant, 2005
- TROPER Michel et CHAGNOLLAUD Dominique (dir.), *Traité international de droit constitutionnel*, Tome 1, Dalloz, 2012
- TUSSEAU Guillaume, *Les normes d'habilitation*, Dalloz, 2006

2. Articles scientifiques

BRUNET Pierre, « Michel Troper et la "théorie" générale de l'État. État général d'une théorie », *Revue française de théorie juridique*, 2003, n° 37, p. 87-110

CARBONNIER Jean, « La religion, fondement du droit ? » in *Droit et religion*, Archives de Philosophie du Droit, tome 38, Sirey, 1993, p. 17-21

CATALA Pierre, « Ebauche d'une théorie juridique de l'information », *Recueil Dalloz*, 1984, p. 97-104

DUONG Lê-My, « Les sources du droit d'internet : du modèle pyramidal au modèle en réseau », *Recueil Dalloz*, 2010, p. 783s.

DWORKIN Ronald, « The Model of Rules », *University of Chicago Law Review*, vol. 35, 1967, p. 14-46

MIAILLE Michel, « La critique du droit », *Droit et Société*, n° 20/21, 1992, p. 80

OST François et VAN DE KERCHOVE Michel, « De la pyramide au réseau ? Vers un nouveau mode de production du droit ? », *Revue Interdisciplinaire d'études juridiques*, vol. 44, 2000, p. 1-82

ROSS Alf, « Tû-Tû », *Harvard Law Review*, vol. 70, 1957, p. 812-825

SULLIVAN Michael et SOLOVE Daniel J., « Can Pragmatism Be Radical ? Richard Posner and Legal Pragmatism », *The Yale Law Journal*, vol. 113, 2003, p. 687-741

TROPER Michel, « Ross, Kelsen et la validité », *Droit et société*, n° 50, 2002, p. 43-57

TUSSEAU Guillaume, « Sur le métalangage du comparatiste », *Revus*, n° 21, 2013, p. 91-115

Histoire d'internet

FLICHY Patrice, « Internet ou la communauté scientifique idéale », *Réseaux*, n° 97, 1999, p. 79-120

HAFNER Katie et LYON Matthew, *Where Wizards Stay Up Late: The Origins of The Internet*, Simon & Schuster International, 1998

Laboratoire Lincoln du MIT, « SAGE: Semi-Automatic Ground Environment Air Defense System », sur *ll.mit.edu* [site web du Laboratoire Lincoln du Massachusetts Institute of Technology]

MARKOFF John, *What the Dormhouse said. How the Sixties Countercultures Shaped the Personal Computer Industry*, New York, Penguin Book, 2006

PUGH Emerson W., *Building IBM: Shaping and Industry and its Technology*, The MIT Press, 1995

Fonctionnement technique d'internet

1. Ouvrages scientifiques

- ATELIN Philippe et DORDOIGNE José, *Réseaux informatiques*, Editions ENI, 2006
- CRUMLISH Christian (informaticien), *The ABC's of the Internet*, Sybex, 1996
- HYDE Randall, *Write Great Code, vol.1: Understanding the Machine*, 2e ed., No Starch Press, 2020
- KUMAR A. Anand, *Fundamentals of Digital Circuits*, 4e ed., PHI Learning, 2016
- LALITTE Éric, *Apprenez le fonctionnement des réseaux TCP/IP*, 4^e éd., Eyrolles, 2019
- PUJOLLE Guy, *Les réseaux. L'ère des réseaux cloud et de la 5G*, 9^e édition, Eyrolles, 2018

2. Articles, cours et interventions scientifiques

- BELOUADHA Fatima-Zahra et EL EULDJ Mohsine, « Architecture des ordinateurs », sur *EMI.ac.ma* [site web de l'École Mohammadia d'ingénieurs à Rabat], 2010-2011
- EL MRABET Nadia, « Les concepts fondamentaux de la cryptographie » [en ligne], conférence à l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) de Rabat, Maroc, *École des Mines de Saint-Étienne*, semaine du 8 au 14 mars 2010
- GBÈTOHO SAHO Nelson Josas, EZIN C. Eugène, « Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm », *CARI 2020 - Colloque Africain sur la Recherche en Informatique et en Mathématiques Appliquées*, Oct 2020, Thiès, Senegal
- KILBURN T., EDWARDS D. B. G., LANIGAN M. J. et SUMNER F. H., « One-Level Storage System », *IRE Transactions on Electronic Computers*, EC-11, 1962, p. 223-235
- KNUDSEN Lars R. et MATHIASSEN John E., « Preimage and Collision Attacks on MD2 », *Fast Software Encryption (FSE)*, 2005, p. 255-267
- MEROLA Antonio, « Utilisation et abus sur le protocole ICMP », *Hakin9*, n° 2, 2006, p. 44-55
- MEYER R. A. et SEAWRIGHT L. H., « A virtual machine time-sharing system », *IBM Syst. J.*, 9, 1970, p. 199-218
- PAYET Pierre, DOUPÉ Adam, KRUEGEL Christopher et VIGNA Giovanni, « EARs in the Wild : Large-Scale Analysis of Execution After Redirect Vulnerabilities », *SAC '13: Proceedings of the 28th Annual ACM Symposium on Applied Computing*, mars 2013, p. 1792-1799
- ROGAWAY Philip et SHRIMPTON Tom, « Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage

Resistance, and Collision Resistance », *Fast Software Encryption (FSE)*, vol. 3017, 2004, p. 371-388

SHANNON Claude, « A Mathematical Theory of Communication », *The Bell System Technical Journal*, vol. 27, juil-oct. 1948, p. 379-423, 623-656

Souveraineté des États et internet

Ouvrages scientifiques

1.

BELLANGER Pierre, *La souveraineté numérique*, Stock, 2014

CAVANAGH A., *Sociology in the Age of the Internet*, McGraw-Hill Education, 2007, p. 41-49

ITEANU Olivier, *Quand le digital défie l'État de droit*, Eyrolles, 2016

NEGRI Antonio et HARTDT Michael, *Multitude: War and Democracy in the Age of Empire*, Penguin Books, 2004

TÜRK Pauline et VALLAR Christian (dir.), *La souveraineté numérique. Le concept, les enjeux*, Mare & Martin, 2017

VENTRE Daniel, *La guerre de l'information*, Paris, Lavoisier, 2007

VENTRE Daniel, *Cyberguerre et guerre de l'information*, Paris, Lavoisier, 2010

2. Articles et rapports scientifiques

BENHAMOU Bernard et SORBIER Laurent, « Souveraineté et réseaux numériques », *Politique étrangère*, 2006, p. 519-530

BOYLE James, « Foucault in Cyberspace », *Yale Journal of Law and Technology*, vol. 2, 2000, p. 177-205

BYK Christian, « L'ère du numérique conduit-elle à l'émergence de nouveaux acteurs et formes de souveraineté ? », *Cahiers Droit, Sciences & Technologies*, n° 15, 2022, p. 171-192

DARNIS Jean-Pierre, « La souveraineté technologique européenne, une réponse à la crise de la Covid-19 ? » [en ligne], *Fondation pour la Recherche Stratégique*, n° 41, mai 2020

DICKINSON Rob, « Transformation of the Modern State: States Sovereignty and Human Rights in the Internet Age », *Connecticut Journal of International Law*, vol. 29, 2013, p. 51-68

EDLER Jakob, BLIND Knut, FRIETSCH Rainer, KIMPELER Simone, KROLL Henning, LERCH Christian, REISS Thomas, ROTH Florian, SCHUBERT Torben, SCHULER Johanna et WALZ Rainer, « Technology sovereignty: from demand to concept » [en ligne], *Fraunhofer Institute for Systems and Innovation Research ISI*, 2020

GANASCIA Jean-Gabriel, GERMAIN Éric et KIRCHNER Claude, « La souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs » [en ligne], *Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene*, oct. 2018

GU Hongfei, « Data, Big Tech, and the New Concept of Sovereignty » [en ligne], *Journal of Chinese Political Science*, mai 2023

HARDY Trotter, « The Proper Legal Regime for "Cyberspace" », *University of Pittsburgh Law Review*, vol. 55, 1994, p. 993-1055

HUMMEL Patrik, BRAUN Matthias, TRETTER Max and DABROCK Peter « Data sovereignty: A review » [en ligne], *Big Data & Society*, vol. 8, janvier-juin 2021

JOHNSON David R. et POST David G., « Law and Borders – the Rise of Law in Cyberspace », *Stanford Law Review*, vol. 48, 1996, p. 1367-1402

KIM Nancy S. et TELMAN Jeremy, « Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent », *Missouri Law Review*, vol. 80, 2015, p. 723-770

PERRITT Henry H. Jr, « Cyberspace and State Sovereignty », *Journal of International Legal Studies*, vol. 3, 1997, p. 155-204

TÜRK Pauline, « La souveraineté des États à l'épreuve d'internet », *Revue du droit public et de la science politique en France et à l'Étranger*, n° 6, 2013, p. 1489s.

TÜRK Pauline, « Définition et enjeux de la souveraineté numérique », sur *Vie-publique.fr*, 2020

VELLIET Mathilde, « Souveraineté numérique : politiques européennes, dilemmes américains » [en ligne], *Institut français des relations internationales*, janv. 2023

WEI Yuxi, « China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty » [en ligne], *The Henry M. Jackson School of International Studies*, 21 juin 2016

WU Timothy, « Cyberspace Sovereignty ? The Internet and the International System », *Harvard Journal of Law and Technology*, vol. 10, 1997, p. 647-666

Gouvernance des noms de domaine

BRICTEUX Caroline, *Régulation de l'Internet par les noms de domaine. Le régime juridique et institutionnel de l'ICANN*, Thèse de droit, Université libre de Bruxelles, 2021

DU MARAIS Bertrand, « Le service public du nommage, consécration et limites », *Revue française d'administration publique*, n° 146, 2013, p. 299-312

MANARA Cédric, « Nom des personnes publiques et droit de l'Internet », *Communication Commerce Electronique*, n° 3, 2016

MASSIT-FOLLÉA F., MÉADEL Cécile et MONNOYER-SMITH Laurence (dir.), *Normative Experience in Internet Politics*, Presse des Mines, 2012

PELLET Alain, « Une gestion privée de l'ordre public de l'internet ? », in PELLET A. (dir.), *Internet et le droit international*, Colloque de Rouen, Editions A. Pedone, 2013, p. 239-249

Contrôle socio-technique d'internet et rapports de force socio-numériques sur internet

AGOSTINELLI Serge, AUGÉY Dominique et LAURIE Frédéric (dir.), *La richesse des réseaux numériques*, Presses Universitaires d'Aix-Marseille, 2012

BASDEVANT Adrien et MIGNARD Jean-Pierre, *L'Empire des données*, Don Quichotte, 2018

FAYON David, *Géopolitique d'Internet*, Economica, 2013

GOLDSMITH Jack L. et WU Tim, *Who Controls the Internet: Illusions of a Borderless World*, Oxford University Press, 2006

HES Ronald, BORKING John J., « Privacy-Enhancing Technologies: The Path to Anonymity », *Information and Privacy Commissioner of Ontario*, 1995

LOVELUCK Benjamin, *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Armand Colin, 2015

MERCKLÉ Pierre, *Sociologie des réseaux sociaux*, La Découverte, 2016

MOREL Camille, *L'État et le réseau mondial de câbles sous-marins de communication*, Thèse de droit de l'université de Lyon, 2020

MOUNIER Pierre, *Les Maîtres du réseau*, La Découverte, 2002

MUELLER Milton L., *Ruling the Root. Internet Governance and the Taming of Cyberspace*, MIT Press, 2002

MUSIANI Francesca, *Nains sans géants : architecture décentralisée et services Internet*, Presses de l'École des mines, Paris, 2013

VIDAL Geneviève (dir.), *La sociologie des usages. Continuités et transformations*, Lavoisier, 2012

WU Tim, « Application-Centered Internet Analysis », *Virginia Law Review*, vol. 85, 1999, p. 1163-1204

WU Tim, « Network Neutrality, Broadband Discrimination », *Journal on Telecom and High Tech Law*, vol. 2, 2003, p. 141-175

WU Tim, « When Code Isn't Law », *Virginia Law Review*, vol. 89, 2003, p. 679-751

Pouvoir expressif sur internet

1. Ouvrages scientifiques

ARLETTAZ Jordane et LE BOT Olivier (dir.), *La démocratie en un clic*, L'Harmattan, 2010

CARDON Dominique, *La démocratie Internet*, Seuil-La République des Idées, 2010

GERBAUDO Paolo, *Tweets and the Streets: Social Media and Contemporary Activism*, Pluto, 2012

HABERMAS Jürgen, *Théorie de l'agir communicationnel* (1981), Fayard, trad. fr. 1987 (t. I) et 1997 (t. II)

HARVEY Pierre-Léonard, *La démocratie occulte. Rapports de force, gouvernance et communautaire dans la société de l'information*, Presses de l'Université Laval, 2004

KREBS Viola, *Le Cybervolontariat : sociopragmatique d'une activité citoyenne au XXI^e siècle*, 2014

SHIRKY Clay, *Here Comes Everybody: How Change Happens when People Come Together*, Penguin, 2008

SUNSTEIN Cass, *Republic.com*, Princeton University Press, 2001

TUFEKÇI Zeynep, *Twitter and Tear Gas : The Power and Fragility of Networked Protest*, YUP, 2017

WOLTON Dominique (sociologue), *Penser la communication*, Flammarion, 1997

WOLTON Dominique, *Internet et après ?*, Flammarion, 1999

2. Articles scientifiques

BERTHOU Renaud « La "forumisation" du droit : à propos des perspectives et enseignements d'une expérience originale de création du droit », *Droit et Société*, n° 61, 2005, p. 783-816

CHALLE Édouard, « Jürgen Habermas et le fondement communicationnel du droit », *Le Philosophoire*, n° 9, 1999, p. 175-199

DESCOMBES Vincent, « Le contrat social de Jürgen Habermas », *Le Débat*, n° 104, 1999, p. 37-44

MAROCCIA Michel, « La normalisation des comportements communicatifs sur internet : étude sociopragmatique de la netiquette » in GUÉGEN Nicolas et TOBLIN Laurence (dir.), *Communication, société et internet*, L'Harmattan, 1998, p. 15-22

MATTELART Armand et MATTELART Michèle, *Histoire des théories de la communication*, La Découverte, 2018

PHILLIPS Whitney, « LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online », *First Monday* [en ligne], vol. 16, 2011

« Le numérique, nouvel objet du droit constitutionnel », *Les Nouveaux Cahiers du Conseil constitutionnel* (NCC), n° 57, 2017

Approches économiques d'internet et (biens) communs

1. Approches économiques d'internet

ANCIAX Arnaud, FARCHY Joëlle et MÉADEL Cécile, « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* n° 158, 2017/2, p. 9-41

ARTHUR W. Brian, « Competing Technologies, Increasing Returns, and Lock-In by Historical Events », *The Economic Journal*, vol. 99, 1989, p. 116-131

BOURREAU Marc, PERROT Anne, « Plateformes numériques : réguler avant qu'il ne soit trop tard », *Notes du Conseil d'Analyse économique*, 2020, n° 60, p. 1-12

COLIN Nicolas, LANDIER Augustin, MOHNEN Pierre et PERROT Anne, « Economie numérique », *Notes du Conseil d'Analyse économique*, 2015, n° 26, p. 1-12

CURIEN Nicolas, FAUCHART Emmanuelle, LAFOND Gilbert, LAINÉ Jean, LESOURNE Jacques, MOREAU François, « Forums de consommation sur Internet. Un modèle évolutionniste », *Revue économique*, vol. 52, 2001, p. 119-135

FARBER Daniel C., « Expressive commerce in cyberspace : public goods, network effects, and free speech », *Georgia State University Law Review*, 2000

JOHNSON David, CRAWFORD Susan et PALFREY John, « The Accountable Internet », *Virginia Journal of Law & Technology*, vol. 9, 2004, p. 1-33

JOLLIVET Pascal, « Les rendements croissants », *Revue Multitudes*, n° 2, 2000, p. 95-96

LAUDON Keneth C., « Markets and privacy », *Communications of the ACM*, 1996, p. 92-104

MOULIER-BOUTANG Yann, *Le Capitalisme Cognitif : La Nouvelle Grande Transformation*, Amsterdam, 2008

PÉNARD Thierry, « L'accès au marché dans les industries de réseau », *Revue internationale de droit économique*, t. XVI, Association internationale de droit économique, 2002, p. 293-312

PÉNARD Thierry, « Faut-il repenser la politique de la concurrence sur des marchés internet ? », *Revue internationale de droit économique*, 2006/1, p. 57-88

PÉNARD Thierry et RALLET Alain, « De l'économie des réseaux aux services en réseaux », *Réseaux*, n° 184-185, 2014, p. 71-93

RALLET Alain, ROCHELANDET Fabrice, ZOLYNSKI Célia, « De la Privacy by Design à la Privacy by Using : regards croisés droit/économie », *Réseaux*, n° 189, 2015/1, p. 15-46

ROCHELANDET Fabrice, *Économie des données personnelles et de la vie privée*, Repères, 2010

ROCHET Jean-Charles et TIROLE Jean, « Platform competition in Two-sided Markets », *Journal of the European Economic Association*, vol. 1-4, 2003, p. 990-1029

SHAPIRO Carl, VARIAN Hal R., *Information Rules*, Harvard Business School Press, 1999

VON HIPPLE Eric, « Democratizing Innovation », *MIT Press*, 2005

2.

Biens communs et internet

Biens communs : un circuit ouvert, Juris associations, n° 501, 2014

BENKLER Yochai, « From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access », *Federal Communications Law Journal*, vol. 52, 2000, p. 561-579

BENKLER Yochai, *The Wealth of Networks. How Social Production Transforms Markets and Freedom*, 2006

BOYLE James, « The Second Enclosure Movement and the Construction of the Public Domain », *Law and Contemporary Problems*, vol. 66, 2003, p. 34-74

BOYLE James, *The Public Domain. Enclosing the Commons of the Mind*, Yale University Press, 2008

BROCA Sébastien et CORIAT Benjamin, « Le logiciel libre et les communs », *Revue internationale de droit économique*, 2015, p. 265-284

CARDON Dominique, *Culture numérique*, Presses de Sciences Po, 2019 (notamment p. 111s.)

CLÉMENT-FONTAINE Mélanie, « Internet et la résurgence des communs » in PARANCE Béatrice et DE SAINT VICTOR Jacques (dir.), *Repenser les biens communs*, CNRS, 2014, p. 261s.

CORIAT Benjamin, « L'idéologie propriétaire a atteint ses limites », *Libération*, 2015

CORNU Marie, ORSI Fabienne, ROCHFELD Judith (dir.), *Dictionnaire des biens communs*, PUF, 2017

FARCHY Joëlle, « Numérique : "Il faut un écosystème de partage des données soutenable sur le long terme" », *Le Monde*, 2018

HARDIN Garrett, « The Tragedy of the Commons », *Science*, vol. 162, 1968, p. 1243-1248

HESS Charlotte et OSTROM Elinor (dir.), *Understanding Knowledge as a Commons*, MIT Press, 2007

HUNTER Dan, « Cyberspace as Place and the Tragedy of the Digital Anticommons », *California Law Review*, vol. 91, 2003, p. 439-519

LESSIG Lawrence, *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, 2001

OSTROM Elinor, *Governing the Commons : The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990

ROCHFELD Judith et SICHEL Olivier, « Nos données nous appartiennent », *Le Monde*, 2015

ZIMMERMANN Jean-Benoît, « La musique à l'heure de l'Internet : du patrimoine aux communs ? » in CORIAT Benjamin (dir.), *Le retour des communs : la crise de l'idéologie propriétaire*, Les liens qui Libèrent, 2015

Normativité endogène au réseau

1. Ouvrages scientifiques

BADOUARD Romain, *Les Nouvelles Lois du web*, Seuil-La République des Idées 2020

BAMDÉ Aurélien, *L'architecture normative du réseau internet. Esquisse d'une théorie*, L'Harmattan, 2014

FLICHY Patrice, *L'imaginaire d'Internet*, La Découverte, 2001

HARVEY David John, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age*, Bloomsbury/Hart Publishing, 2017

LESSIG Lawrence, *Code: Version 2.0*, Basic Books, 2006

MATHIAS Paul, *Des libertés numériques*, PUF, 2008

O'NEIL Cathy, *Weapons of Math Destruction*, Crown Books, 2016

PALOQUE-BERGÈS Camille, *Poétique des codes sur le réseau informatique*, Archives Contemporaines, 2009

PASQUALE Frank, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015

SIMON Herbert, *Administrative Behavior*, Macmillan, 1947

SIMONDON Gilbert, *Du mode d'existence des objets techniques*, 2012, Aubier

STIEGLER Bernard, *La technique et le temps. Tome 3. Le temps du cinéma et la question du mal-être*, Galilée, 2001

STIEGLER Bernard, *La société automatique. 1. L'avenir du travail*, Fayard, 2015

TURKLE Sherry, *The Second Self : Computers and the Human Spirit*, HarperCollins, 1984

TURKLE Sherry, *Life on the Screen: Identity in the Age of the Internet*, Simon & Schuster, 1995

2. Articles et témoignages scientifiques

BARDINI Thierry et PROULX Serge, « La culture du hack en ligne, une rupture avec les normes de la modernité », *Les Cahiers du numérique*, vol. 3, 2002, p. 35-54

COHEN Julie, « Cyberspace as/and Space », *Columbia Law Review*, vol. 107, 2007, p. 210-256

GODEFROY Lémy D., « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz*, n° 8, 2016, p. 438-444

GRANAI George, « André Leroi-Gourhan, A. - Evolution et techniques. Vol. I : L'homme et la matière ; Vol. II : Milieu et techniques ; B. - Archéologie du Pacifique nord » in *Revue de géographie de Lyon*, vol. 26, n°4, 1951, p. 461-463

GUCHET Xavier, « Evolution technique et objectivité technique chez Leroi-Gourhan et Simondon » [sur *Open Edition*], *Appareil*, n° 2, 2008

HARRIS Tristan, « How a Handful of Tech Companies Control Billions of Minds every day ? », Conférence sur *Ted.com*, avr. 2017

HARRIS Tristan, « How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist », sur *Medium.com*, mai 2016

HARVEY Pierre-Léonard, *Design communautaire appliqué aux systèmes sociaux numériques. Fondements communicationnels, théories et méthodologies*, Presses de l'Université du Québec, 2014

JOHNSON David et POST David, « And How Shall the Net be Governed ? » in KAHIN Brian et KELLER James H. (dir.), *Coordinating the Internet*, MIT Press, 1997, p. 62-91

JURGENSON Nathan, « When Atoms Meet Bits : Social Media, the Mobile Web and Augmented Revolution », *Future Internet* 4, n° 1, 2012, p. 83-91

POPLIN François, « André Leroi-Gourhan et le monde animal » in Collectif CNRS., *André Leroi-Gourhan ou les Voies de l'Homme*, Actes du colloque du CNRS (mars 1987), Albin Michel, 1988, p. 51-60

REIDENBERG Joel, « Governing Networks and Rule-Making in Cyberspace », *Emory Law Journal*, vol. 45, 1996, p. 912-930

ROUVROY Antoinette et BERNS Thomas, « Gouvernamentalité algorithmique et perspectives d'émancipation », *Réseaux*, n° 177, p. 163-196

STIEGLER Bernard, « Questions de pharmacologie générale. Il n'y a pas de simple pharmakon », *Psychotropes*, 2007, vol. 13, p. 27-54

TURKLE Sherry, « Seeing Through Computers », *The American Prospect*, 2001

TURKLE Sherry, « L'écran fragmenté », *Sociétés*, n° 79, 2003, p. 17-34

Transhumanisme et intelligence artificielle

BOSTROM Nick, « A History of Transhumanist Thought », *Journal of Evolution and Technology*, vol. 14, 2005

BOSTROM Nick, *Superintelligence*, Dunod, 2017

BOSTROM Nick et SANDBERG Anders, *Whole Brain Emulation. A Roadmap*, 2008

CHRAIBI KAADOUH Ikram et GARENNE André, « Architecture des réseaux de neurones: Réseaux de neurones artificiels classiques (2/3) ! », sur *Scilogs.fr*, 2018

DAMOUR Franck, « Le mouvement transhumaniste. Approches historiques d'une utopie technologique contemporaine », *Vingtième Siècle. Revue d'Histoire*, n° 138, 2018, p. 143-156

ETTINGER Robert, *The Prospect of Immortality*, 1962

ETTINGER Robert, *Man into Superman*, 1972

GANASCIA Jean-Gabriel, *Le Mythe de la Singularité. Faut-il craindre l'intelligence artificielle ?*, Seuil, 2017

HUXLEY Julian, *New Bottles for New Wine*, Chatto & Windus, 1957

MCCARTHY John, MINSKY Marvin, ROCHESTER Nathaniel et SHANNON Claude, « A proposal for the Dartmouth Summer Research Project on Artificial Intelligence », 31 août 1955 pt. 3

Relations homme-machine

DE CONDORCET Nicolas, « Lettres d'un jeune mécanicien aux auteurs du Républicain », 1791

ELLUL Jacques, *Le Système technicien*, Calmann-Lévy, 1977

GIBSON William, *Neuromancer*, Ace Books, 1984

LE ROUX Ronan, « L'homéostasie sociale selon Norbert Wiener », *Revue d'histoire des sciences humaines*, n° 16, 2007, v. p. 121-124

WIENER Norbert, *The human use of human beings : cybernetics and society*, Houghton Mifflin, 1954

Systèmes et règles internes aux systèmes

ANTOINE Charles, *Introduction à la physique quantique*, Dunod, 2020

BARTHES Roland, « The Death of the Author », *Aspen Magazine*, n° 5/6, 1967

BARTHES Roland, *Le degré zéro de l'écriture*, Seuil, 1953

BERRAH Nora, HUMPHREY Marc, PANCELLA Paul, VAUDREY Catherine, *Physique quantique. Le guide de référence*, Les éditions Trédaniel, 2019

DOSSE François, *Histoire du structuralisme*, La Découverte, 2012 (2 tomes)

FOUCAULT Michel, « Qu'est-ce qu'un auteur », *Bulletin de la Société française de philosophie*, n°3/63^e année, 1969 (conf. de 1968)

POUVREAU David, *Une histoire de la "systémologie générale" de Ludwig von Bertalanffy*, Thèse en histoire des sciences, EHESS, 2013

RABOUIN David, « Chapitre I. Structuralisme et comparatisme en sciences humaines et en mathématiques : un malentendu ? », in MANIGLIER Patrice (dir.), *Le Moment philosophique des années 1960 en France*, PUF, 2011, p. 37-57

VON BERTALANFFY Ludwig, « The history and status of General Systems Theory », in KLIR George (dir.), *Trends in General Systems Theory*, New York, Wiley, 1972, p. 21-41

Régulation : concept, histoire, usages en droit et application à internet **1. Histoire de la régulation**

BERNARD Claude, *Rapport sur les progrès et la marche de la physiologie générale en France*, Imprimerie impériale, 1867

DE SAINT ALBINE Pierre-Raymond, *Mémoire sur le laminage du plomb*, Imprimerie de Pierre Prault, 1731

DESAGULIERS Jean-Théophile, *Cours de physique expérimentale*, Tome 2, J. Rollin, 1751 (v. notamment p. 471s., cours publié en 1727)

La régulation entre sciences de la vie et sciences du gouvernement (XIXe-XXe siècles), Revue Arabes, n° 4, 2008, p. 31

SPENCER Herbert, *The Study of Sociology*, London, H. King & Co, 1873

SULLY Henri, *Règle artificielle du temps*, G. Dupuis, 1737

2. Conceptualisation de la régulation des rapports de force

BRÉCHET Jean-Pierre, « Le regard de la théorie de la régulation sociale de Jean-Daniel Reynaud », *Revue française de gestion*, n° 184, 2008, p. 13-34

CROZIER Michel, « Administration et bureaucratie. Le problème des moyens organisationnels de développement », *Sociologie du travail*, 1962, p. 367-378

CROZIER Michel, *Le phénomène bureaucratique*, Seuil, 1963

CROZIER Michel, « Pouvoir et organisation », *Archives européennes de sociologie*, vol. 5, 1964, p. 52-64

DAHL Robert, « The concept of power », *Behavioral Science*, n° 2, 1957, p. 201-215

DE TERSSAC Gilbert (dir.), *La théorie de la régulation sociale de Jean-Daniel Reynaud*, 2003

FRIEDBERG Erhard, *Le pouvoir et la Règle. Dynamiques de l'action organisée*, Seuil, 1993

REYNAUD Jean-Daniel, *Les règles du jeu. L'action collective et la régulation sociale*, Armand Colin, 1989

WIENER Norbert, *Cybernétique et société*, Paris, Deux Rives, 1952

3. La régulation juridique

BARREAU Jocelyne et MOULINE Abdelaziz, « La déréglementation américaine des télécommunications et l'Europe : les exemples français et britanniques », *Revue d'économie industrielle*, n° 39 1987, p. 170-179

BONNECHÈRE Michèle, « Les tendances à la déréglementation et leur incidence sur la théorie des sources en droit du travail », *Droit social*, n° 1, janv. 1990, p. 40-48

HAZEL François et COMMAILLE J. (dir.), *Normes juridiques et régulation sociale*, Journées d'études 1987, Bordeaux, LGDJ, 1991

CHEVALLIER Jacques, « Décentralisation et politiques publiques », *AJDA*, avr. 1992, p. 120-127

CHEVALLIER Jacques, « La régulation juridique en question », *Droit et société*, n° 49, 2001, p. 827-846

CHEVALLIER Jacques, « L'État régulateur », *Revue française d'administration publique*, n° 111, 2004, p. 473-482

CHEVALLIER Jacques, « Les autorités administratives indépendantes : un produit d'importation ? », in BOTTINI Fabien (dir.), *Néolibéralisme et américanisation du droit*, Mare et Martin, 2019, p. 141-154

COHEN-TANUGI Laurent, « L'État et la déréglementation : les enjeux institutionnels de la déréglementation », *Réseaux*, n° 40, 1990, p. 25-34

EISEMANN Pierre-Michel, « Jacques Naveau. Droit du transport aérien international », *Politique étrangère*, n° 45, 1980, p. 1044-1045

FRISON-ROCHE M.-A., « Le droit de la régulation », *Recueil Dalloz*, fév. 2001, p. 610-617

FRISON-ROCHE M.-A., « Le droit, source et forme de régulation mondiale », in JACQUET Pierre, PISANI-FERRY Jean et TUBIANA Laurence (dir.), *Gouvernance mondiale*, La Documentation française, 2002, p. 313-330

LAVERGNE Benjamin, *Recherche sur la soft law en droit public français*, Thèse en droit public, Toulouse, PUF, 2013

ROUBAN Luc, « Évaluation des politiques publiques et mouvement de dérégulation aux États-Unis », *Revue française d'administration publique*, n° 29, 1984, p. 85s

TEITGEN-COLLY Catherine, « Les autorités administratives indépendantes, histoire d'une institution », in COLLIARD Claude-Albert et TIMSIT Gérard, *Les autorités administratives indépendantes*, PUF, 1988

4. Applications de la régulation juridique à internet

BELLI Lucas, *De la gouvernance à la régulation de l'internet*, Thèse de droit, Berger-Levrault, 2016

MAISL Herbert, « La régulation des télécommunications, changements et perspectives », *RFDA*, mai 1995, p. 449s.

FRISON-ROCHE Marie-Anne (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016

Régulation d'internet en France

1. Ouvrages et articles scientifiques

ALAUZEN Marie, « L'État plateforme et l'identification numérique des usagers », *Réseaux*, n° 212, 2019, p. 211-239

BLAIZOT-HAZARD Catherine, « Savoir et droits fondamentaux – De l'ère industrielle à l'ère communicationnelle », *RFDA*, n° 4, 2016, p. 707s.

BOSSAN Jérôme, « Le droit pénal confronté à la diversité des intermédiaires de l'internet », *Revue de science criminelle et de droit pénal comparé*, 2013 (pages ?)

DERIEUX Emmanuel, « Responsabilité du "producteur" d'un service de communication au public en ligne : condition d'une fixation préalable », *La revue européenne des médias et du numérique*, n°20, automne 2011

HE Linxin, « La sécurité sociale à l'ère du numérique : quel renouveau de la solidarité ? », *Revue de droit sanitaire et social (RDSS Dalloz)*, p. 301-318

KESTEMAN Nadia, « Entre illettrisme et illectronisme. Les nouveaux publics à faible autonomie administrative », *Revue des politiques sociales et familiales*, n° 135, 2020, p. 65-73 ;

MATTATIA Fabrice, *Droit d'auteur & propriété intellectuelle dans le numérique*, Eyrolles, 2017

PELLEGRINI François et CANEVET Sébastien, *Droit des logiciels*, PUF, 2013

PONTIER Jean-Marie, « Lutte contre l'illectronisme ? », *AJDA*, 2020, p. 2225-2228

2. Presse et associations

CONDOMINES Anaïs, « On a discuté avec des détenus sur Facebook : "Toute la taule a un smartphone" », sur *TF1info.fr*, oct. 2017

DE PASQUALE Anthony, « Les prisonniers français sont sur Snapchat », sur *Vice.com*, fév. 2016

TÔN Emilie, « Prison: "Presque chaque détenu possède un portable, certains en ont plusieurs" », *L'Express*, 2016

UTERSINGER Martin et REYNAUD Florian, « Les adresses Telegram bloquées en France par erreur », *Le Monde*, 13 mai 2023

« Le portable en prison : mobile d'évasion », *M le magazine du Monde*, sept. 2012

« L'État entend rester "un des principaux actionnaires d'Orange", assure Hollande », sur *Les Echos*, 8 juin 2016

« Des détenus se filment sur Snapchat fumant un joint », *La Dépêche*, juil. 2018

« Béziers: des détenus mettent une annonce sur Snapchat pour trouver des "jeteurs" », *Le Figaro*, juil. 2019

Observatoire international des prisons, « Fracture numérique : les prisons, une "zone blanche" » [en ligne], *Revue Dedans-Dehors*, n° 113, déc. 2021

3. Lois

Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications

Loi n° 2001-624 du 17 juillet 2001 portant diverses dispositions d'ordre social, éducatif et culturel

Loi n° 2003-1365 du 31 décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle

Loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique

Loi n° 1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique

Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense

Loi n° 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière

Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République

Loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique

Loi n° 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet

4. Règlements

Note du 21 mai 2004 intitulée Interdiction faite aux détenus d'accéder à internet et à tout [système d'information (SI)] extérieur

Circulaire NOR/LBL/B/04/10062/C du 28 juillet 2004, « Fonds de compensation pour la TVA »

Circulaire de la Direction de l'Administration pénitentiaire relative à l'accès à l'informatique pour les personnes placées sous main de justice du 13 octobre 2009, NOR : JUSK094006C

Arrêté du 29 avril 2013 relatif à l'approbation du cahier des charges de l'appel à projets « France très haut débit - Réseaux d'initiative publique »

Cahier des charges de l'appel à projets « France Très Haut Débit - Réseaux d'initiative publique », 2013

Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

Décret n° 2017-677 du 28 avril 2017 portant diverses dispositions relatives à la régulation des jeux en ligne, art. 2

5. Décisions de justice

TGI Paris, ord., *UEJF, LICRA et MRAP c/ Yahoo! Inc. et Yahoo France*, 20 nov. 2000

TGI Paris, ord., *PMU c/ Computer Aided Technologies*, 2 nov. 2005

TGI Nanterre, Juge des référés, 10 juillet 2008, n° 08/01490

TGI Paris, ord., *UEJF c. Twitter*, 24 janv. 2013

TGI Paris, ord., *APC e. a. c/ Auchan Telecom e. a.*, 8 nov. 2013

TGI Paris, réf., *Allostreaming*, 28 nov. 2013

TGI Paris, 3^e ch. 2^e sect., *Zone Téléchargement et autres*, 15 déc. 2017, n° 17/13471

TGI Paris, 3^e ch. 2^e sect., *Filmstreamvk e. a.*, 25 mai 2018, n° 18/03028

TGI Paris, réf., *FNDF e. a. c/ Orange e. a.*, 13 juillet 2018, n° 18/55236

TGI Paris, 3^e ch. 2^e sect., *FNDF e. a. c/ Google Inc., Bouygues Telecom e. a.*, 14 déc. 2018, n° RG 18/10652

CA Paris, 4^e ch. Sect. A, *Google France c. Louis Vuitton*, 28 juin 2006

CA Montpellier, 5^e ch. sect. A, *Jean-Marc D. c/ JFG Networks*, 15 déc. 2011

CA Paris, Pôle 05 ch. 7, 19 déc. 2013, n° 2012/19484

CA Paris, 1^{ère} ch. Pôle 5, *Allostreaming*, 15 mars 2016, n° 040/2016

C. Cass., *Allostreaming*, 6 juil. 2017, n° 16-17.217

CC, *Loi modifiant la loi du 30 sept. 1986 relative à la liberté de communication*, 17 janv. 1989, n° 88-248 DC

CC, *Hadopi I*, 10 juin 2009, n° 2009-580 DC

6. Documents des administrations et autorités habilitées par l'État

Autorité de régulation des télécommunications, « Réponse de l'Autorité de régulation des télécommunications à la consultation publique relative à l'évolution du droit français des communications électroniques » [en ligne sur *Arcep.fr*], 2002

Autorité de régulation des télécommunications, « Adapter la régulation au nouveau contexte du marché des télécommunications », Rapport, juil. 2002

Autorité de régulation des télécommunications, Avis du Comité d'Experts du 17 mai 2005 concernant l'autorisation de la technique READSL2 au répartiteur dans le cadre de l'accès à la boucle locale de France Télécom

Arcep, Avis n° 2007-0745 du 20 septembre 2007 relatif à la demande d'avis du Conseil de la concurrence portant sur la demande de mesures conservatoires déposée par la société Free relative à des pratiques de la société France Télécom sur le secteur des infrastructures de génie civil dans le secteur des communications électroniques

Arcep, Avis n° 2018-0101 du 30 janvier 2018 sur des dispositions relatives à la sécurité et à la défense des systèmes d'information dans le cadre du projet de loi relatif à la programmation militaire pour les années 2019-2025

Autorité française de la concurrence, Décision n° 08-D-02 du 12 février 2008 relative à une demande de mesures conservatoires présentée par la Free SAS et concernant l'accès aux infrastructures de génie civil de France Télécom dans le cadre du déploiement de boucles locales optiques résidentielles de type FTTh

Arcep, Décision n° 2008-0835 du 24 juillet 2008 portant sur la définition du marché pertinent de gros des offres d'accès aux infrastructures physiques constitutives de la boucle locale filaire, sur la désignation d'un opérateur exerçant une influence significative sur ce marché et sur les obligations imposées à cet opérateur sur ce marché

Arcep, « Mise en œuvre de l'accès à la sous-boucle et articulation avec le développement du très haut débit », oct. 2009

Arcep, Décision n° 2009-1106 du 22 décembre 2009 précisant, en application des articles L. 34-8 et L. 34-8-3 du code des postes et des communications électroniques, les modalités de l'accès aux lignes de communications électroniques à très haut débit en fibre optique et les cas dans lesquels le point de mutualisation peut se situer dans les limites de la propriété privée

Arcep, Décision n° 2010-1312 du 14 décembre 2010 précisant les modalités de l'accès aux lignes de communications électroniques à très haut débit en fibre optique sur l'ensemble du territoire à l'exception des zones très denses

Arcep, avis n° 2011-1241 du 20 oct. 2011 répondant à la demande d'avis de l'Autorité de la concurrence portant sur la saisine de la société Cogent en date du 9 mai 2011 relative à des pratiques mises en œuvre par la société France Télécom sur le marché du transit et ses marchés connexes

Arcep, Observatoire des marchés des communications électroniques, « Services fixes haut et très haut débit (marché de détail) », 28 fév. 2013

Arcep, « Observatoire Haut et Très Haut Débit : abonnements et déploiements. Les chiffres du 4^{ème} trimestre 2017 », m^{ai} le 8 mars 2018

Arcep, « L'accès haut débit via l'ADSL », mis à jour en juin 2018

Arcep, « "New Deal" mobile », 25 oct. 2018

Arcep, « Marché des communications électroniques en France – Les chiffres au 4^{ème} trimestre 2021 », m^{ai} le 7 avril 2022

Arcep, Observatoire des marchés des communications électroniques, « Les services de communications électroniques en France. 1^{er} trimestre 2022 », 7 juil. 2022

Arcep, « Marché du haut et du très haut débit fixe. Les abonnements à la fibre optique désormais majoritaires en France », Communiqué de presse, 8 sept. 2022

Arcep, « Le partage de réseaux mobiles » [en ligne], mis à jour le 8 déc. 2022

Arcep, « Marché des communications électroniques en France – Les chiffres au 4^{ème} trimestre 2022 », mäj le 6 avr. 2023

Arcep, « Les obligations de déploiement des opérateurs », mis à jour le 30 mai 2023

Arcep, « L'état d'internet en France. Rapport d'activité », juil. 2023

Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022

Conseil d'État, Rapport « Internet et les réseaux numériques », 1998

Conseil d'État, Rapport « Le numérique et les droits fondamentaux », 2014

Conseil de la concurrence, Avis n° 2002-A-04 du 11 avril 2002 relatif à l'acquisition par la société Télédiffusion de France d'un ensemble de sites pylônes de la société Bouygues Telecom

Hadopi, « Hadopi, biens culturels et usages d'Internet : pratiques et perceptions des internautes français – BU 4 », sur *Hadopi.fr*, janv. 2014

Hadopi, « Rapport d'activité 2015-2016 », 10 janv. 2017

Hadopi, « Étude sur les risques encourus sur les sites illicites », juin 2017

Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2017 – BU 7 », sept. 2017

Hadopi, « Biens culturels et usages d'internet : pratiques et perceptions des internautes français 2018 – BU8 », avr. 2018

Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2019 », déc. 2019

Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2020 », févr. 2021

Hadopi, « Baromètre de la consommation de biens culturels dématérialisés 2021 », nov. 2021

Hadopi, « L'Essentiel n°3 », 3 sept. 2017, p. 4. Pour l'évolution du nombre d'abonnés aux services de musique en streaming : Arcom, « Baromètre de la consommation des biens culturels dématérialisés 2022 », déc. 2022

Sénat français, « L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne », Rapport d'information n°696, 8 juil. 2014

Régulation d'internet au Royaume-Uni

1. Ouvrages et articles scientifiques

AKDENIZ Yaman, « The Regulation Of Pornography And Child Pornography On The Internet. », *Journal of Information, Law and Technology*, 1997, p. 1-36

GERLI Paolo, WAINWRIGHT David et WHALLEY Jason, « Infrastructure investment on the margins of the market », *Telecommunications Policy*, 41, 2017

IGLEZAKIS Ioannis, *The Legal Regulation of Cyber Attacks*, Kluwer Law International B.V., 2020

THONIER Axel, « Dix ans de réforme des télécommunications au Royaume-Uni : échec du pilotage de la structure de marché et libéralisation complète », *Économie & prévision*, 1995, p. 107-125

VAN GORP Annemijn F., MAITLAND Carleen F. et HANEKOP Heidemarie, « The broadband Internet access market », *Telecommunications Policy*, vol. 30, 2006

VINCENT James, « BT to introduce default “porn filtering” » [en ligne], *The Independent*, 16 déc. 2013

WESTAWAY Luke, « Sky Broadband to start filtering adult content by default » [en ligne], sur *CNET*, 20 janv. 2015

2. Presse

CHAMPEAU Guillaume, « Près de 20 % des sites les plus populaires sont bloqués en GB », *Numerama*, 4 juil. 2014

HUGHES Matthew, « Ofcom says no price controls on full-fibre broadband until 2031, giving BT's Openreach the kick to 'build like fury' », *The Register*, 18 mars 2021

JACKSON Mark, « Virgin Media UK Trial Deep Packet Inspection to Track Illegal File Sharing » [en ligne], sur *ISPReview UK*, 2009

JACKSON M., « Gov Starts GBP5bn UK Gigabit Broadband and Voucher Schemes UPDATE », *ISP Review*, 19 mars 2021

JACKSON Mark, « Ofcom Begin New Review of UK Net Neutrality Rules Post Brexit UPDATE » [en ligne], sur *ISPReview UK*, 7 sept. 2021

LAUSSON Julien, « Le Royaume-Uni essaie une nouvelle fois de forcer les sites pornos à vérifier l'âge des internautes », *Numerama*, 8 fév. 2022

REES Marc, « UK : Wikipédia piquée par l'un des scorpions du filtrage », *NextInPact*, 8 déc. 2008

« Sites pornographiques : cinq questions sur "l'attestation numérique" que le gouvernement envisage d'instaurer pour bloquer l'accès aux mineurs », *France Info*, 6 fév. 2023

3.

Lois

Copyright, Designs and Patents Act (1988)

Minister of State for Energy, E-Commerce and Postal Services, Department of Trade and Industry, *The Electronic Communications (Universal Service) Order*, 2003

Wireless Telegraphy Act (2006)

4. Documents des autorités étatiques ou habilitées par l'État

BROWN Thomas, « Digital Economy Act 2017 (Commencement of Part 3) Bill [HL] », sur *Lordslibrary.parliament.uk* [site web de la Bibliothèque de la chambre des Lords], 19 janv. 202

Department for Business Innovation & Skills et Department for Culture, Media & Sport, « Digital Britain. Final Report », juin 2009

Department for Science, Innovation & Technology et Department for Culture, Media & Sport, « BDUK Broadband Delivery Project », 9 mars 2011

Department for Digital, Culture, Media & Sport, « Broadband Delivery Programme: Delivery Model », sept. 2011

Department for Digital, Culture, Media & Sport et DOWDEN Oliver, « Government launches new £5bn "Project Gigabit" » (communiqué de presse), 19 mars 2021

Oftel, « National roaming », 16 sept. 2003

Oftel, *Annual report 2003*, 10 déc. 2003

Ofcom, « Coverage and planning policy for analogue radio broadcasting services », 2 mars 2005

Ofcom, « Universal Service Obligation », 10 janvier 2005-21 mars 2005

Ofcom, « Retail Price Controls », 19 juil. 2006

Ofcom, *Wireless Telegraphy Act Licensing. Terms, Provisions and Limitations*, 2011

Ofcom, *Ofcom's approach to net neutrality*, 24 nov. 2011

Ofcom, « 3G Coverage Obligation Verification Methodology », 9 mai 2012

Ofcom, « The availability of communications services in the UK », mai 2013

Ofcom, « Review of the wholesale broadband access markets », juin 2014

Ofcom, « Designing the broadband universal service obligation », avr. 2016

Ofcom, « Connected Nations 2016 », 16 déc. 2016

Ofcom, « Connected Nations 2017 », 15 déc. 2017

Ofcom, « Connected Nations 2018 », 18 déc. 2018

Ofcom, « Coverage obligations in the 700 MHz and 3.6-3.8 GHz spectrum award. Ofcom's approach to verifying compliance », 31 janv. 2019

Ofcom, *Ofcom's approach to assessing compliance with net neutrality rules. Frameworks for assessing zero rating offers and traffic management measures for compliance with the Open Internet Regulation*, 16 mai 2019

Ofcom, « Connected Nations 2019 », 20 déc. 2019

Ofcom, *Improving spectrum access for Wi-Fi. Spectrum use in the 5 and 6 GHz bands*, janv. 2020

Ofcom, « Connected Nations 2020 », 19 déc. 2020

Ofcom, *Interface Requirements IR 2030 – Licence Exempt Short Range Devices*, 2021

Ofcom, « Connected Nations 2021 », 16 déc. 2021

Ofcom, « Connected Nations 2022 », 15 déc. 2022

Ofcom, « UK Home Broadband Performance », oct. 2022 ; Arcep, « L'état d'internet en France. Edition 2023 », juil. 2023

Régulation d'internet aux États-Unis

1. Ouvrages et articles scientifiques

DALY Angela, « The Legality of Deep Packet Inspection », *International Journal of Communications Law and Policy*, vol. 14, 2011

ESCORNE Charlotte, « Les enjeux de la neutralité du Net aux États-Unis », *Hérodote*, n° 177-178, 2020, p. 215-234

FU Chuan, ZHANG Guoqing, YANG Jing et LIU Xiaona, « Study on the contract characteristics of Internet architecture », *Enterprise Information Systems*, vol. 5, Taylor & Francis, 2011, p. 495-513

JOYCE Craig P. et PATTERSON L. Ray, « Copyright in 1791: An essay Concerning the Founders' View of the Copyright Power Granted to Congress in Article I, Section 8, Clause 8 of the US Constitution », *Emory Law Journal*, vol. 52, 2003

MATWYSHYN Andrea M., « Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction through Data Privacy », vol. 98, *Northwestern Law Review*, p. 493-544

MUELLER Milton L. et ASGHARI Hadi, « Deep packet inspection and bandwidth management », *Telecommun. Policy*, 36, 2012., p. 462–475

ROSS SUNHAM Catherine, « Zippo-ing the Wrong Way : How the Internet Has Misdirected the Federal Courts in Their Personal Jurisdiction Analysis », *University of San Fransisco Law Review*, vol. 43, p. 559-584

ST. AUBIN Christopher et STOCKING Galen, « Key facts about Gab », *Pew Research Center*, 24 janv. 2023

THIEL David, DIRESTA Renée, GROSSMAN Shelby et CRYST Elena, « Contours and Controversies of Parler », *Stanford Internet Observatory*, 28 janv. 2021

UPPALURI Anusha, *A Two-market Inter-ISP Contracting Framework*, Thèse d'informatique, UMI, 2011

WALTHER Samantha et MCCOY Andrew, « US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism », *Perspectives on Terrorism*, vol. 15, avr. 2021, p. 100-124

2. Presse et associations

REES Marc, « Pédopornographie : 84 000 sites bloqués et accusés par erreur » [en ligne], *NextInPact*, 17 févr. 2011

KELLEY Jason et MACKEY Aaron, « KOSA Would Let the Government Control What Young People See Online » [en ligne], *Electronic Frountier Foundation*, nov. 2022

KELLEY Jason, MACKEY Aaron, « Dangerous "Kids Online Safety Act" Does Not Belong in Must-Pass Legislation », *Electronic Frountier Foundation*, déc. 2022

3. Lois

Copyright Act (1790)

Clayton Act (1914)

Communications Act (1934)

Children's Online Privacy Protection Rule (COPPA, 1998)

Public Law 105-277 du 21 oct. 1998

Clarifying Lawful Overseas Use of Data Act (CLOUD ACT, 2018)

Kids Online Safety Act (projet de loi)

Device Filter Amendments, H.B. 72, 23 mars 2021 (Amendement de l'Utah)

Sensitive Materials in Schools, H.B. 374, 24 mars 2022 (Amendement de l'Utah)

4. Décisions de justice

Cour Suprême des États-Unis, *Reno v. ACLU*, 521 U.S. 844 (1997)

Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. aux pts 1119-1123 (W.D. Pa. 1997)

GTE New Media Services Inc. v. Bellsouth Corp., 199 F.3d 1343 (2d Cir. 2000)

Nyabwa v. Facebook, CIVIL ACTION NO. 2:17-CV-24 (S.D. Tex. Jan. 26, 2018)

Knight Institute v. Donald Trump, No 17 Civ. 5205 (NRB) (S.D.N.Y. May 23, 2018)

Cour fédéral du District Sud de New-York, *United King Distributors et al. v. Israeli-tv.com et v. Israel.tv*, No 1:2021cv11025, 26 avr. 2022

5. Documents des administrations et autorités habilitées par l'État

FCC, *Equipment Authorization. Approval Guide* [en ligne], oct. 2015

FCC, *Unlicensed Use of the 6 GHz Band; Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz*, FCC-20-51, avr. 2020

Régulation d'internet en Chine

1. Ouvrages et articles scientifiques

ARSÈNE Séverine, *Internet et politique en Chine. Les contours normatifs de la contestation*, Karthala, 2011

ARSÈNE Séverine, « Complexité du nationalisme numérique en Chine », *Perspectives chinoises*, n° 2020-2, juin 2020

BANDURSKI David, « China's Guerrilla War for the Web », *Far Eastern Economic Review*, vol. 171, juil. 2008, p. 41s.

BAO Han, « "Rice Bunnies" – #MeToo in China: A hashtag movement and women's empowerment through social media », *Conference: Proceedings of EVA London*, juil. 2019

BAYEN-POISSON Aurélie « Cybercontrôle en Chine : l'omni-surveillance à l'ère du numérique » [en ligne], *La Revue des Médias*, 21 déc. 2018

BRANSTETTER Lee G., « Does "Made in China 2025" work for China ? Evidence from Chinese listed firms », *National Bureau of Economic Research*, nov. 2022, 34 p.

CAO Cong, « L'industrie chinoise face au défi technologique », *Perspectives chinoises*, n° 83, mai-juin 2004

CAO Cong, « Chine », in *Rapport de l'UNESCO sur la science : vers 2030*, 2016, p. 620-641

CLAYTON Richard, MURDOCH Steven et WATSON Robert, « Ignoring the Great Firewall of China », *Privacy Enhancing Technologies*, 2006, p. 20-35

HAN Rongbin, *Challenging the Regime, Defending the Regime: Contesting Cyberspace in China*, Thèse en sciences politiques, Université de Californie, Berkeley, 2012

HOANG Nguyen Phong, NIAKI Arian Akhavan, DALEK Jakub, KNOCKEL Jeffrey, LIN Pellaeon, MARCZAK Bill, CRETE-NISHIHATA Masahi, GILL Phillipa et POLYCHRONAKIS Michalis, « How Great is the Great Firewall? » [en ligne sur arXiv], *30th USENIX Security Symposium*, 2021, p. 3381-3398

KING Gary, PAN Jennifer et ROBERTS Margaret E., « How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument », *American Political Science Review*, vol. 111, 2017, p. 484-501

KNOCKEL Jeffrey, PARSONS Christopher, RUAN Lotus, XIONG Ruohan, CRANDALL Jedidiah et DEIBERT Ron, « We Chat, They Watch. How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus », sur *Citizenlab.ca*, 7 mai 2020

LONG Fei et LIU Yunchuan, « Fake Sales and Ranking Algorithms in Online Retail Marketplace with Sponsored Advertising », *Social Science Research Network*, 2022

NOAM Eli M., *Who Owns the World's Media?*, Oxford University Press, 2016, p. 758s.

RICHERI Guseppe, « L'Internet en Chine, entre État et opinion publique », *Les Enjeux de l'information et de la communication*, n° 19, 2018, p. 21-33

SACHWALD Frédérique, « La Chine, puissance technologique émergente », *Institut français des relations internationales (IFRI)*, juin 2007

TAN Zixiang (Alex), FOSTER William et GOODMAN Seymour, « China's state-coordinated Internet infrastructure », *Communications of the ACM*, vol. 42, 1999, p. 44-52

TANG Chao, « In-depth analysis of the Great Firewall of China » [en ligne], *COMPT 116*, 2016

YAN Jiayi, « Hashtag activism, feminist counterpublics, and the myth of intersectionality: a case study of the emerging online discourse on Weibo #Feng County sex-trafficking case », Université de Liverpool, *Academia.edu*, 2022

WANG Hao, « The conceptual basis of privacy standards in China and its implications for China's privacy law », *Frontiers of Law in China*, vol. 7, 2012, p. 134-160

- WANG Jiangyu, « The State As Controlling Shareholder in Chinese State-Owned Enterprises », *SSRN Electronic Journal*, 2018
- WANG Jing, « Sustainability of China's anti-monopoly law in the digital era: an observation on the 'choosing one from two' jurisprudence from China », Paper presented at 19th Asian Law Institute Conference, Tokyo, Japan, 2022
- WANG Raymond, « China », *The Technology, Media and Telecommunications Review*, ed. 13, 6 janv. 2023 [en ligne sur *Thelawreviews.co.uk*]
- WINTER Philipp et LINDSKOG Stefan, « How the Great Firewall of China is Blocking Tor » [en ligne], *USENIX -FOCI'12*, 2012
- WU Xiaobo, *The Story of Tencent: Evolution of Chinese Internet Companies from 1998 to 2016. The Evolution of the Chinese Internet Company*, Zhejiang University Press, 2017
- WÜBBEKE Jost, MEISSNER Mirjam, ZENGLEIN Max J., IVES Jacqueline et BJÖRN Conrad, *Made in China 2025. The making of a high-tech superpower and consequences for industrial countries*, Mercator Institute for China Studies, 12 août 2016
- YANG Feng, The tale of deep packet inspection in China: Mind the gap, *3rd International Conference on Information and Communication Technology*, 2015
- ZENG Jing, « #MeToo as connective action: A study of the anti-sexual violence and anti-sexual harassment campaign on Chinese social media in 2018 », *Journalism Practice*, vol. 14, 2020, p. 171-190
- ZHANG Ge, LI Zhao, HUANG Jiaming, WU Jia, ZHOU Chuan et YANG Jian, « eFraudCom: An E-commerce Fraud Detection System via Competitive Graph Neural Networks », *ACM Transactions on Information Systems*, vol. 40, juil. 2021
- ZHANG Karen, « The promises and pitfalls of digital activism: Fighting for #MeToo under the Great Firewall of China », *ANU Undergraduate Research Journal*, vol. 11, n° 1, avr. 2021
- ZHAO Jing (ANTI Michael), « Behind the Great Firewall of China », Conférence TED sur *ted.com*, juin 2012
- ZHOU Shuhuan, « Status and Risk Factors of Chinese Teenagers' Exposure to Cyberbullying », *Sage Open*, vol. 11, oct. 2021
- ZITTRAIN Jonathan et EDELMAN Benjamin, « Empirical Analysis of Internet Filtering in China » [en ligne], *Berkman Center for Internet & Society*, Harvard Law School, 2003
- « China Aims for Global Leadership in Robotics with new 5-year Plan », *International Federation of Robotics*, janv. 2022
- « China: Robot installations grew by 44 percent », *International Federation of Robotics*, sept. 2022

« Ask the Experts: Is China's Semiconductor Strategy Working? » [en ligne], *Blogs LSE* [London School of Economics], sept. 2022

2. Presse et associations

BOYD Alexander et YU Alex, « Inside peng shuai's accusation against former top leader: #metoo, censorship, and resistance discourse », *China Digital Times*, 4 nov. 2021

CAO Aowen et FENG Emily, « The mystery of the chained woman in China », *NPR*, 17 fév. 2022

CHANG CHIEN Amy et STEVENSON Alexandra, « 'Where is **?': Fans in China Elude Censors to Talk About Peng Shuai », *The New York Times*, 2 déc. 2021

CIMPANU Catalin, « Oracle: China's internet is designed more like an intranet », sur *ZDNet*, 23 juil. 2019

DAVIDSON Helen, « The disappearance of Peng Shuai: what happened to the Chinese tennis star? », *The Guardian*, 19 nov. 2021

DEFRANOUX Laurence, « #MeToo en Chine : une star du tennis accuse de viol un ancien vice-Premier ministre », *Libération*, 3 nov. 2021

DORNEL Nelly, « Comment les manifestants chinois contournent l'IA des réseaux sociaux », *Huffington Post*, déc. 2022

GAN Nectar et XIONG Yong, « Chinese tennis star accuses former top Communist Party leader of sexual assault, triggering blanket censorship », *CNN*, 17 nov. 2021

GERTZ Bill, « China blocks U.S. from cyber warfare », *The Washington Times*, 12 mai 2009

LEPLÂTRE Simon, « Le plan "Made in China 2025" visé par les taxes américaines », *Le Monde*, 5 avr. 2018

NIVELLE Pascale, « "Caonima", le clip qui fait la nique à Pékin », *Libération*, 16 mars 2009

SCHAEFFER Frédéric, « Industrie : l'Europe s'inquiète des ambitions de la Chine », *Les Echos*, 8 mars 2017

SHEN Xinmei, « Popular TV show reveals how WeChat crushed a rival messaging app » [en ligne], sur *South China Morning Post*, 12 nov. 2018

YUN Wang, « Les fonctionnaires réduisent au silence les demandes d'enquête émanant de civils. Les gens descendront-ils dans la rue par solidarité avec la mère des huit enfants ? » (官媒噤声民间推动调查 人们会上街声援八孩母亲 ?), *Radio Free Asia*, 16 fév. 2022

« Des nouilles pho et des pandas. Comment les internautes en Chine inventent un langage pour contourner la censure liée au COVID-19 », *Amnesty International*, 6 mars 2020

3. Lois et réglementations

Conseil des affaires de l'État, Dispositions provisoires pour la gestion de la connexion internationale des réseaux informatiques (中华人民共和国计算机信息网络国际联网管理暂行规定), 1^{er} fév. 1996

Conseil des affaires de l'État, Règlement sur la sécurité de la République populaire de Chine, la protection et la gestion des réseaux d'information et d'Internet (计算机信息网络国际联网安全保护管理办法) du 30 déc. 1997

Conseil des affaires de l'État de la République populaire de Chine, Décret n° 292 « Mesures relatives à l'administration des services d'information sur Internet » (互联网信息服务管理办法), 25 sept. 2000

Conseil des affaires de l'État, Règlement sur les télécommunications (中华人民共和国电信条例), 25 sept. 2000

Conseil des affaires de l'État, Règlement de la République populaire de Chine sur les télécommunications (中华人民共和国电信条例) du 25 sept. 2005

Loi Anti-Monopole de la République populaire de Chine du 1^{er} août 2008

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services de recherche d'informations sur internet (互联网信息搜索服务管理规定) du 25 juin 2016

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services d'information pour les applications mobiles sur internet (移动互联网应用程序信息服务管理规定) du 28 juin 2016

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services de diffusion en direct sur internet (互联网直播服务管理规定) du 4 nov. 2016

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services pour les forums et communautés sur internet (互联网论坛社区服务管理规定) du 25 août 2017

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services de commentaire sur internet (互联网跟帖评论服务管理规定) du 25 août 2017

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des services d'information des groupes sur internet (互联网群组信息服务管理规定) du 7 sept. 2017

Administration du cyberspace de la Chine, Dispositions relatives à l'administration des informations sur les comptes publics des utilisateurs d'internet (互联网用户公众账号信息服务管理规定) du 7 sept. 2017

Administration du cyberspace de la Chine, Avis sur les dispositions relatives à l'administration des services de commentaire sur internet (projet de révision publiquement soumis aux commentaires des internautes) (互联网跟帖评论服务管理规定 (修订草案征求意见稿)) du 17 juin 2022

Ministère chinois du Commerce, Catalogue des technologies encouragées à être importées en Chine (中国鼓励引进技术目录) du 18 déc. 2006

Ministère chinois du Commerce, Opinions directrices pour encourager la digestion, l'absorption et la ré-innovation des technologies importées (关于鼓励引进技术消化吸收再创新的指导意见) du 16 déc. 2010

4. Décisions de justice

奇虎公司与腾讯公司垄断纠纷上诉案 [Qihoo 360 v. Tencent], 2013 SUP. PEOPLE'S CHINA CIVIL JUDGMENT No. Minsanzhongzi 4/2013

Régulation d'internet en Russie

1. Ouvrages, articles et études scientifiques

Centre Levada, « Internet, Réseaux sociaux et VPN » (Интернет, социальные сети и VPN), sur *Levada.ru*, avr. 2022

Centre Levada, « Les principales sources d'information des Russes » (Основные источники информации россиян), sur *Levada.ru*, nov. 2022

Centre Levada, « Principales sources d'information et journalistes populaires » (Основные источники информации и популярные журналисты), sur *Levada.ru*, avr. 2023

Centre Levada, « Audience des réseaux sociaux et des messageries » (Аудитория социальных сетей и мессенджеров), sur *Levada.ru*, avr. 2023

Centre Levada, « Conflit avec l'Ukraine » (Конфликт с Украиной), sur *Levada.ru*, 31 mars 2022

Centre Levada, « Conflit avec l'Ukraine : évaluation de mai 2023 » (Конфликт с Украиной: оценки мая 2023 года), *Levada.ru*, 1^{er} juin 2023

BOZALKA Dusan, « Guerre en Ukraine : comment la Russie s'appuie sur la sphère complotiste pour diffuser sa propagande », *La Revue des médias*, 24 avr. 2023

CHUPIN Ivan et MUSTAFINA Renata, « Quand le geste révèle le militant : sur quelques cas d'entrée en journalisme d'opposition dans la Russie contemporaine », *Critique Internationale*, n°79, 2018, p. 159-179

LIMONIER Kevin, « Vers un « Runet souverain » ? » [en ligne], *EchoGéo* n° 56, Pôle de recherche pour l'organisation et la diffusion de l'information géographique (CNRS UMR 8586), août 2021

PARIS Gilles, « Comment des "trolls" russes ont réussi à peser sur l'élection présidentielle américaine » [en ligne], *Le Monde*, 2018

PIGMAN Lincoln, « In memoriam: Russia's ban on Telegram, 2018-2020 », *Riddle Russia*, 22 juin 2020

RICHTER Andrei et RICHTER Anya, *Réglementation des contenus en ligne en Fédération de Russie?*, Observatoire européen de l'audiovisuel, 2015

VITALIY Lapshichyov, « Technology of Deep Packet Inspection for recognition and blocking traffic of the Tor network » [en ligne], *XII International Conference on Security of Information and Networks*, Sotchi 2019

WIJERMARS Mariëlle et LEHTISAARI Katja, *Freedom of Expression in Russia's New Mediasphere*, Routledge, 2019

ZAKHAROVA Maria et PAUTHE Nicolas, « La liberté de la presse et des médias en Russie », *Droit et Société*, n° 93, 2016, p. 437-452

« Content Restrictions on TikTok in Russia following the Ukrainian War », sur *Tracking.exposed* [association de chercheurs], 13 avr. 2022

2. Presse

BATEMAN Tom, « TikTok's ban on foreign content in Russia 'risks turning it into a propaganda platform' », sur *Euronews.com*, 17 mars 2022

BALASHOVA Anna, KUZNETSOVA Evgeniya, POSYPKINA Alexandra, « La Russie, rien que la Russie : quels sont les risques du projet sur le Runet souverain? » (РФ и точка: какие риски несет проект о суверенном Рунете) [en ligne], *RBC*, 15 déc. 2018

BEARDSWORTH James, « Explainer: Who Are Russia's Pro-War Bloggers And Why Are They Important? », *The Moscow Times*, 15 sept. 2022

BURGESS Matt, « This is why Russia's attempts to block Telegram have failed », *Wired*, 28 avr. 2018

CHANG Gordon G., « China's TikTok Is Russia's New Disinformation Machine », *Newsweek*, 25 mars 2022

GILBERT David, « Russian TikTok Influencers Are Being Paid to Spread Kremlin Propaganda », sur *Vice.com*, 11 mars 2022

FEDOROVA Maria, « Tiktoker universel. Ce que font les blogueurs six mois après le blocage de l'application TikTok en Russie » (Универсальный тиктокер. Чем занимаются блогеры спустя полгода после блокировки приложения TikTok в России), *Nasha Versia* (média russe indépendant), 5 nov. 2022

GAVRILYUK Anastasia, « Le blocage se renforce » (Блок крепчает), *Kommersant.ru*, mars 2022

IGNATIEV Dmitry, « L'audience d'Instagram a été divisée par 5 en un an de blocage, tandis que celle de Facebook a été divisée par 3,5 » (За год блокировки аудитория Instagram упала в 5 раз, а Facebook – в 3,5 раза), *Vedomosti*, 4 mars 2023

KASHEVSKY Valery, « La Russie a-t-elle réussi à créer un substitut aux réseaux sociaux étrangers ? » (Получилось ли у России создать замену иностранным соцсетям?), sur *Eurasianet.org*, 1^{er} déc. 2022

KEFFER Laura, « Telegram dépasse WhatsApp en termes de volume de trafic en Russie » (Telegram обогнал WhatsApp по объему трафика в России), *Kommersant*, 23 janv. 2023

LELOUP Damien, « TikTok accusé d'offrir un "passe-droit" aux propagandistes du Kremlin », *Le Monde*, 15 mars 2022

MEAKER Morgan, « Why WhatsApp Survived Russia's Social Media Purge », *Wired*, 21 mars 2022

NAST Condé, « Russia's Internet Censorship Machine Is Going After Tor » [en ligne], *Wired UK*, 2021

OREMUS Will, « TikTok created an alternate universe just for Russia », sur *Washingtonpost.com*, 13 avr. 2022

PANKRATOVA Irina, « Guerre et paix dans TikTok. Comment les "maisons tiktok" russes se sont transformées en bureaux de propagande militaire » (« Война и мир в TikTok. Как российские «тикток-хаусы» превратились в офисы военной пропаганды »), sur *Thebell.io*, 22 juil. 2022

PINNA Monica, « L'exode silencieux des élites culturelles de Russie suite à la guerre en Ukraine », *Euronews*, 21 déc. 2022

POZYCHANYUK Valeria, « TikTok patriotique, Big Techs et censure et premiers signes de récession dans l'informatique » (Патриотичный TikTok, бигтехи и цензура и первые признаки рецессии в IT), *The Bell*, 24 juil. 2022

SHIGAREVA Margarita, « "Certains sont simplement retournés à la besogne" Comment la vie des blogueurs russes a-t-elle changé en un an sans TikTok ? » («Некоторые просто в шарагу пошли обратно» Как изменилась жизнь российских блогеров за год без TikTok?), sur *Lenta.ru* [journal d'État], 9 mars 2023

STOLYAROV Gleb, « Russia starts operation to lay undersea fibre optic cable through Arctic », *Reuters*, 6 août 2021

TOFANYUK Elena et SAPRONOVA Ioulia, « Quelque 700 000 citoyens ont quitté la Russie depuis le 21 septembre » (Россию после 21 сентября покинули около 700 000 граждан), sur *Forbes.ru*, 4 oct. 2022

TOUZANI Samir, « La Russie déplore la fuite de 100.000 employés de la tech », *Les Echos*, 20 déc. 2022

« A Moscow court sanctions the Russian government's request to block Telegram », *Meduza*, 13 avr. 2018

« L'équipement du "RuNet souverain" sera modernisé aux frais de l'État » (Оборудование для "суверенного рунета" модернизируют за счет государства) [en ligne], *Kommersant*, 17. fév. 2020

« Russia lifts ban on Telegram messaging app after failing to block it », *Reuters*, 18 juin 2020

« Le ministère des communications a une nouvelle fois annulé l'exercice dans le cadre de la loi sur le RuNet souverain » (Минцифры вновь отменило учения в рамках закона о суверенном Рунете) [en ligne], *Interfax*, 21 sept. 2020

« Échecs pour l'indépendance. Le trafic se perd dans les équipements du "Runet souverain" » (Сбои за независимость. В оборудовании «суверенного рунета» заблудился трафик) [en ligne], *Kommersant*, 9 avr. 2021

« Le RuNet souverain en cours de retrait de la circulation. Le ministère de l'économie s'oppose aux nouvelles idées du Roskomnadzor » (Суверенный рунет выбивается из трафика. Минэкономики против новых идей Роскомнадзора) [en ligne], *Kommersant*, 20 fév. 2022

« Pourquoi les autorités veulent-elles créer un "RuNet souverain" : de quoi protège-il contre quelles menaces ? » (Зачем власти создают «суверенный Рунет»: от чего он защитит и чем грозит), sur *Trends.rbc.ru*, mis à jour le 28 fév. 2022

« Digital Ministry opposes giving state's stake in Rostelecom to Rostec, sees risks as too high - source », *Interfax*, avr. 2022

« Russia Has Blocked 138K Websites Since Ukraine Invasion, Prosecutor Says », *The Moscow Times*, 8 août 2022

« En Russie, le secteur technologique subit un exode sans précédent », *Courrier International*, 2 mai 2022

3. Lois et règlements

Loi fédérale n° 2124-I relative aux médias de masse (Закон о средствах массовой информации) du 27 décembre 1991

Loi fédérale n° 126 FZ relative aux communications (Федеральный закон о связи), 7 juil. 2003

Loi fédérale n° 149-FZ relative à l'information, aux technologies de l'information et à la protection de l'information ("Об информации, информационных технологиях и о защите информации") du 27 juil. 2006

Loi fédérale n 142-FZ du 14 juin 2011 portant modification de certains textes de loi de la Fédération de Russie en vue d'améliorer la législation applicable au secteur de l'information de masse » (Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового регулирования в сфере средств массовой информации")

Loi fédérale n° 139-FZ modifiant la loi fédérale sur la protection des mineurs contre les l'informations nuisibles à leur santé et à leur développement et certains actes législatifs de la Fédération de Russie ("О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации) du 28 juillet 2012

Loi n°242-FZ du 21 juil. 2014 portant modification de certains actes législatifs de la Fédération de Russie afin de clarifier la procédure de traitement des données à caractère personnel dans les réseaux d'information et de télécommunication (Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях")

Loi fédérale n° 31-FZ modifiant l'article 15.3 de la loi fédérale « sur l'information, les technologies de l'information et la protection de l'information » (Федеральный закон "О внесении изменений в статью 15.3 Федерального закона "Об информации, информационных технологиях и о защите информации") du 18 mars 2019 [Loi pour un internet souverain]

Loi fédérale n° 90 FZ modifiant la loi fédérale relative aux communications et la loi fédérale relative à l'information, aux technologies de l'information et à la protection de l'information du 1^{er} mai 2019 [Loi pour un internet souverain]

Décret fédéral n° 2385 du 30 déc. 2020 relatif aux activités d'octroi de licences dans le domaine des services de communication et à l'invalidation de certains actes du gouvernement de la Fédération de Russie (Постановление Правительства РФ "О лицензировании деятельности в области оказания услуг связи и признании утратившими силу некоторых актов Правительства Российской Федерации »)

Loi fédérale n° 530-FZ du 30 décembre 2020 portant modification de la loi fédérale sur l'information, les technologies de l'information et la protection de l'information

Loi fédérale n° 32-FZ sur les amendements au Code pénal de la Fédération de Russie et aux articles 31 et 151 du Code de procédure pénale de la Fédération de Russie (Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации") du 4 mars 2022

4. Décisions de justice

Tribunal du district de Meschansky (Moscou), aff. n° 5-1794/2017 du 16 oct. 2017

Régulation d'internet en Corée du Nord

1. Contributions scientifiques

BANKS Stacey, « North Korean Telecommunications », *North Korean Review*, 1, McFarland & Company, vol. 1, 2005, p. 88-94

DUFFLEY Robert, « Information Technology and Control in the DPRK » [en ligne], *Cornell International Affairs Review*, vol. 5, 2011, p. 47-53

GRUNOW Florian et SCHIESS Niklas, « Linfting the Fog on Red Star OS. A deep dive into the surveillance features of Nord Korea's operating system » (Conférence-Talk [en ligne]), *Chaos Computer Club*, 2015

PAPAIN Tom, « North Korea and Cyberwarfare: How North Korea's Cyber Attacks Violate the Laws of War », *Journal of Korean Law*, vol. 11, 2011, p. 29-54

RASKA Michael, « North Korea's Evolving Cyber Strategies: Continuity and Change », *SIRIUS – Zeitschrift für Strategische Analysen*, vol. 4, no. 2, 2020, p. 1-13

SELIGER Bernhard et SCHMIDT Stefan, « The Hermit Kingdom Goes Online ... Information Technology, Internet Use and Communication Policy in North Korea », *North Korean Review*, vol. 10, 2014, p. 71-88

WARD Peter et DENNEY Steven, *Information Dissemination in North Korea: A Report for NGOs*, Rapport pour le National Endowment for Democracy (NED), janv. 2022

2. Presse

AHN JH et YORK Rob, « Are PUST students potentiel North korean hackers ? » [en ligne], *NKNews* [journal américain sur l'actualité nord-coréenne], déc. 2015

BOYNTON Robert S., « North Korea's Digital Underground » [en ligne], *The Atlantic*, avr. 2011

CAESAR Ed, « The Incredible Rise of North Korea's Hacking Army » [en ligne], *The New Yorker*, 2021

GREENBERG Andy, « North Korea Hacked Him. So He Took Down Its Internet » [en ligne], *Wired*, 2 fév. 2022

HA Yuna, « Four publicly executed in Pyongyang on charges of distributing "illegal video materials" », *Daily NK*, 12 mars 2021

HAJEK Danny, « Watching Foreign Movies Is Illegal In North Korea, But Some Do It Anyway », *NPR*, 5 juil. 2017

HORNADAY Ann, « Sony, 'The Interview' and the unspoken truth: All movies are political », *Washingtonpost.com*, déc. 2014

JEONG Tae-Joo, « La Corée du Nord demande aux organisations de mettre à jour leurs applications... et vérifie également si des programmes de contournement sont installés » (北, 앱 업데이트 조직적 지시...우회 프로그램 설치 여부도 검열) [en ligne], *Daily NK*, 8 juil. 2022

JI-HYE Jun, « JCS refuses to share new wartime plan with Assembly » [en ligne], *The Korea Times*, oct. 2015

KECK Zachary, « North Korea Bans Wi-Fi for Foreigners », *The Diplomat*, 11 sept. 2014

KIM Jaewon, « North Koreans tap into smartphone apps on restricted state network » [en ligne], *Nikkei*, 6 juin 2019

KO Donghwan, « North Korea's 7 million smartphone users under regime's watchful eye » [en ligne], *The Korea Times*, nov. 2022

LEE Daehee, « Les "hackers d'élite" de la Corée du Nord se livrent à un cyberharcèlement de devises étrangères » (北 '엘리트 해커' 사이버 외화벌이), *Nocutnews.co.kr* [journal sud-coréen], août 2011

LEE Jong-Heon, « Internet cafe opns in N.Korea », *United Press International*, 28 mai 2002

MÄKELÄINEN Mika, « Yle Pohjois-Koreassa: Kurkista suljetun maan omaan tietoverkkoon » (Yle en Corée du Nord : coup d'oeil dans le réseau d'information du pays ermite), *Yle*, 14 mai 2016

MARTIN Bradley K., « North Koreans: Watching foreign movies is "impure" », *Asia Times*, 6 juil. 2022

PAGE Carly, « North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies » [en ligne], *TechCrunch*, août 2022

PEARSON James, « The \$50 device that symbolizes a shift in North Korea », *Reuters*, 27 mars 2015

RYALL Julian, « Why is North Korea 'cracking down' on "foreign influence" ? », *Deutsche Welle*, 8 juin 2021

SANGER David E., KIRKPATRICK David D. et PERLROTH Nicole, « The World Once Laughed at North Korean Cyberpower. No More. » [en ligne], *The New York Times*, oct. 2017

TALMADGE Eric, « North Korea announces blocks on Facebook, Twitter and YouTube » [en ligne], *The Guardian*, 1 avril 2016

TALMADGE Eric, « North Korea's digital divide: Online elites, isolated masses » [en ligne], *Chicago Tribune*, nov. 2017

TIMBERG Craig et NAKASHIMA Ellen, « Not so isolated » [en ligne], *Washington Post*, 25 juil. 2017

UTERSINGER Martin, Le FBI accuse la Corée du Nord du vol de 540 millions de dollars dans le réseau de cryptomonnaie Ronin, *Le Monde*, 15 avr. 2022

WILLIAMS Martyn, « North Korea's Internet Domain Is in New Hands », sur *PCWorld.com*, 19 mai 2011

WILLIAMS Martyn et SCHIESS Niklaus, « Project Reveal. New research into North Korea's digital control system », *Lumen*, avr. 2022

« North Korea slaps Wi-Fi ban on embassies and NGOs » [en ligne], *The Korea Times*, 11 sept. 2014

« Selfies and surveillance: North Korea's new connectivity » [en ligne], *Bangkok Post*, 10 novembre 2017

« South Korean intelligence says N. Korean hackers possibly behind Coincheck heist » [en ligne], *Reuters*, 5 fév. 2018

« The Lazarus heist: How North Korea almost pulled off a billion-dollar hack » [en ligne], *BBC*, juin 2021

« Le FBI accuse la Corée du Nord d'avoir piraté le jeu de cryptomonnaies « Axie Infinity », *Courrier International*, 15 avr. 2022

3.

Lois et réglementations

Code pénal nord-coréen

4. Associations et autorités officielles

Département de l'Armée des États-Unis, *North Korean Tactics* [rapport en ligne], Army Techniques Publications No. 7-100.2, juil. 2020

Healthcare Sector Cybersecurity Coordination Center (HC3), « North Korean Cyber Activity » [en ligne]. *U.S. Department of Health & Human Services*, mars 2021, p. 14

WILLIAMS Martyn, « Digital Trenches. North Korea's Information Counter-Offensive » [en ligne], *Committee for Human Rights in North Korea (HKRN)*, 2019

WILLIAMS Martyn, « North Korea Intensifies War Against Foreign Influence », *38 North*, 10 nov. 2021

« North Korea: Connection Denied: Restrictions on mobile phones and outside information in North Korea »[en ligne], *Amnesty International*, 9 mars 2016

Régulation juridique d'internet dans l'Union européenne

1. Ouvrages et articles scientifiques

OCHOA Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Thèse de droit, HAL, 2014

CURIEN Nicolas, « La libéralisation des télécommunications en Europe », *Flux*, n° 44-45, 2001, p. 28-35

DEZOBRY Guillaume, *La théorie des facilités essentielles*, LGDJ, Bibliothèque de droit international et communautaire

2. Presse

REES Marc, « Le Digital Services Act expliqué ligne par ligne (articles 1 à 24) », *NextInPact*, 4 janv. 2021

REES Marc, « Le Digital Services Act expliqué ligne par ligne (articles 25 à 74) », *NextInPact*, 6 janv. 2021

3. Programmes de l'Union européenne

« Télécommunications », *Revue du marché commun*, n° 284, fév. 1985, p. 120

Commission européenne, Livre vert sur le développement du marché commun des services et équipements de télécommunications, 30 juin 1987, COM/87/290 final

4. Réglementations

Directive 90/388/CEE de la Commission du 28 juin 1990 relative à la concurrence dans les marchés des services de télécommunication

Directive 91/250 du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur

Directive 96/19/CE du 13 mars 1996 modifiant la directive 90/388/CEE en ce qui concerne la réalisation de la pleine concurrence sur le marché des télécommunications

Directive 97/33/CE du 30 juin 1997 relative à l'interconnexion dans le secteur des télécommunications en vue d'assurer un service universel et l'interopérabilité par l'application des principes de fourniture d'un réseau ouvert

Directive 2000/31/CE

Règlement (CE) n° 2887/2000 du Parlement européen et du Conseil du 18 décembre 2000 relatif au dégroupage de l'accès à la boucle locale

Directive 2001/29 sur l'harmonisation du droit d'auteur et des droits voisins dans la société de l'information

Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion

Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques

Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques

Directive 2002/22 du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques

Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public

Règlement (UE) n ° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (Règlement eIDAS)

Règlement européen 2015/2120 dit « pour l'accès à un Internet ouvert »

Directive 2019/790 du 17 avr. 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique (Directive « Damun »)

Règlement 2021/1232 du 14 juil. 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne

Règlement 2022/2065 du 19 oct. 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (*Digital Service Act*, ou « DSA »)

Proposition de Règlement du Parlement européen et du Conseil du 15 décembre 2020 relatif aux marchés contestables et équitables dans le secteur numérique, COM(2020) 842 final

5. Décisions de justice

CJUE, Gde ch., *Google France c. LVMH*, 23 mars 2010, aff. C-236/08

CJUE, Gde ch., *L'Oréal c. eBay*, 12 juil. 2011, aff. C-324/09

CJUE, *Google Spain et Google Inc. c/ AEPD*, 13 mai 2014, n° 131/12

CJUE, Gde ch., *Maximillian Schrems c/ Data Protection Commissioner*, C-362/14, 6 oct. 2015

CJUE, *GC e. a. c/ CNIL*, 24 sept. 2019, n° C-136/17

CJUE, *Google LLC c/ CNIL*, 24 sept. 2019, n° C-507/17

CJUE, *Data Protection Commissioner c/ Maximillian Schrems*, 16 juil. 2020, C-311/18

CJUE, *Telenor Magyarország préc.*, 15 sept. 2020, aff. C-807/18

CJUE, *Pologne c. Parlement européen et Conseil de l'Union européenne*, 26 avr. 2022, aff. C-401/19

CJUE, *TU, RE c/ Google LLC*, 8 déc. 2022, n° C-460/20, §68 et 72

Régulation juridique d'internet dans le Conseil de l'Europe

Cour EDH, *Handyside*, 7 déc. 1976, n° 5493/72

Cour EDH, 4^e sect., *Times Newspapers Ltd c. Royaume-Uni (n°s 1 et 2)*, 10 mars 2009, n° 3002/03 et 23676/03

Cour EDH, *Axel Springer c/ Allemagne*, 7 fév. 2012, n° 39954/08

Cour EDH, *Ahmet Yildirim c. Turquie*, 18 déc. 2012, n° 3111/10

Cour EDH, 5^e sect., *Ashby Donald e. a. c. France*, 10 janv. 2013, n° 36769/08

Cour EDH, Gde ch., *Delfi AS c. Estonie*, 16 juin 2015, n° 64569/09

Cour EDH, *Cengiz e. a. c. Turquie*, 1^{er} déc. 2015, n° 18226/10 et 14027/11

Cour EDH, *OOO Flavus and others versus Russia*, n° 12468/15, 23 juin 2020, 23489/15 et 19074/16

Cour EDH, *Hurbain c/ Belgique*, 22 juin 2021, n° 57292/16

Cour EDH, *Biancardi c/ Italie*, 25 nov. 2021, n° 77419/16

Études mathématiques et expérimentales sur internet

BAVELAS Alex, « A mathematical model for group structures », *Applied Anthropology*, 7, Society for Applied Anthropology, 1948

CASILLI Antonio, « Être présent en ligne : culture et structure des réseaux sociaux d'Internet », *Idées économiques et sociales*, n° 169, 2012, p. 16-29

COHEN Edith, DELLING Daniel, PAJOR Thomas et WERNECK Renato F., « Computing Classic Closeness Centrality, at Scale » [en ligne], *Proceedings of the second edition of the ACM conference on Online social networks - COSN '14*, août 2014

DANG NGUYEN Godefroy et LETHIAIS Virginie, « Impact des réseaux sociaux sur la sociabilité. Le cas de Facebook », *Réseaux*, n° 195, 2016, p. 165-195

DIUK Carlos, « The Formation of Love », sur *Facebook.com*, 11 fév. 2014, étude pour le compte de Facebook

FAN Rui, ZHAO Jichang, CHEN Yan et XU Ke, « Anger is More Influential Than Joy: Sentiment Correlation in Weibo », *ArXiv*, 10 sept. 2013

FREEMAN Linton C., « A Set of Measures of Centrality Based on Betweenness », *Sociometry*, vol. 40, American Sociological Association, *Sage Publications*, 1977, p. 35-41

HAO Karen, « How Facebook got addicted to spreading misinformation » [en ligne], *MIT Technology Review*, 11 mars 2021

HANSEN Derek L., SHNEIDERMAN Ben, SMITH Marc A. et HIMELBOIM Itai, *Analyzing Social Media Networks with NodeXL (Second Edition)*, Morgan Kaufmann, 2020

HOYLE Roberto, DAS Srijita, KAPADIA Apu, LEE Adam J. et VANIEA Kami, « Was my message read?: Privacy and Signaling on Facebook Messenger » in *CHI'17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, p. 3838-3842

JARDINE Eric, LINDNER Andrew et OWENSON Gareth, « The potential harms of the Tor anonymity network cluster disproportionately in free countries » [en ligne], *Proceedings of the National Academy of Sciences*, vol. 117, déc. 2020

LITTMAN Rebecca et LEVY PALUCK Elizabeth, « The Cycle of Violence: Understanding Individual Participation in Collective Violence », *Political Psychology*, vol. 36, fév. 2015, p. 76-99

MARTEL Cameron et RAND David G., « Misinformation warning labels are widely effective : A review of warning effects and their moderating features », *Current Opinion in Psychology*, vol. 54, déc. 2023

MATHEW Binny, ILLENDULA Anurag, SAHA Punyajoy, SARKAR Soumya, GOYAL Pawan, MUKHERJEE Animesh, « Hate begets Hate: A Temporal Study of Hate Speech », *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, p. 1-24

MILLI Smitha, CARROLL Micah, SASHRIKA Pandey, WANG Yike et DRAGAN Anca D., « Twitter's Algorithm: Amplifying Anger, Animosity, and Affective Polarization », *ArXiv*, 26 mai 2023

NIMMO Ben, « Measuring Traffic Manipulation on Twitter » [en ligne], *Oxford Internet Institute*

OWEN Gareth et SAVAGE Nick, « The Tor Dark Net » [en ligne], *Centre for International Governance Innovation*, sept. 2015

RIEDER Bernhard, MATAMOROS-FERNÁNDEZ Ariadna et COROMINA Òscar, « From ranking algorithms to "ranking cultures": Investigating the modulation of visibility in YouTube search results », *Convergence*, vol. 24, p. 50-68

ROBERTS Hal, LAROCHELLE David, FARIS Robert et PALFREY John, « Mapping Local Internet Control » [en ligne], *Berkman Center for Internet & Society*, 2011

ROBERTS Hal, ZUCKERMAN Ethan, FARIS R., YORK Jillian et PALFREY J., *The Evolving Landscape of Internet Control* [en ligne], Berkman Center for Internet & Society, août 2011

ROGERS Richard, « Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media », *European Journal of Communication*, vol. 35, 6 mai 2020, p. 213-229

SALAMATIAN Loqman, DOUZET Frederick, LIMONIER Kevin et SALAMATIAN Kavé, « The geopolitics behind the routes data travels: a case study of Iran », *Journal of Cybersecurity*, vol. 7, 2021 [en ligne sur *arXiv.org*]

SILVA MOTA DRUMOND Gabrielle, COUTANT Alexandre, MILLERAND Florence, « La production de l'usager par les algorithmes de Netflix », *Les Enjeux de l'information et de la communication*, n° 19/2, 2018, p. 29-44

Dictionnaires

CORNU Gérard, *Vocabulaire juridique*, 8e édition, PUF, 2007

Dictionnaire Gaffiot, en ligne sur *Gaffiot.fr*

Dictionnaire du CNRTL, en ligne sur *Cnrtl.fr*

Dictionnaire Larousse, en ligne sur *Larousse.fr*

Dictionnaire Littré, en ligne sur *Littre.org*

Bases de données :

BuiltWith

DNSlytics

IPinfo

iResearch China

Semrush

SimilarWeb

StatCounter

Unilaw.go.kr (base de données du gouvernement sud-coréen recensant les normes juridiques nord-coréennes en vigueur)

Annexe 1. Liste des applications les plus utilisées mondialement au dernier semestre 2022

Dans la liste qui suit, on évalue le nombre d'utilisateurs actifs/mois (*monthly active users*, MAU) des applications selon :

- Le nombre de visiteurs uniques/mois pour : les sites web en principe (sauf pour les exceptions qui seront exposées dans les critères suivants), les moteurs de recherche, les agrégateurs d'actualités, les applications de blogs, pornographiques et les services de fourniture ou de renvoi vers des pages publicitaires (Taboola, Outbrain, Linktree...) ;
- Le nombre d'acheteurs et de vendeurs effectuant au moins une transaction chaque mois, pour les services de commerce en ligne (TaoBao, Amazon, Aliexpress...) ;
- Le nombre d'utilisateurs qui cliquent chaque mois sur une publicité, pour les services de régie publicitaire (Google Ads, Alimama, Meta Business Manager, Microsoft Advertising...) ;
- Le nombre d'utilisateurs qui accèdent à l'application au moins une fois par mois et y consacrent en moyenne plusieurs minutes par jour, pour ce qui est des applications de réseaux sociaux ;
- Le nombre d'utilisateurs qui téléchargent chaque mois des applications ou des mises à jour, pour les magasins d'applications (Play Store, App Store, AppGallery...).

On a indiqué entre parenthèses l'ordre juridique auquel est rattaché le propriétaire de l'application.

Rang	Application en ligne	Nombre d'utilisateurs actifs/mois (MAU) dans le monde en 2022
1	Google Search (US) Moteur de recherche et portail web Propriété d'Alphabet, Inc.	3,5 – 3,7 mds
2	Facebook (US) Réseau social de partage de contenus Propriété de Meta Platform	2,7 – 2,9 mds
3	Chrome (US) Navigateur web Propriété d'Alphabet, Inc.	2,55 – 2,75 mds
4	Play Store (US) Magasin d'applications Propriété d'Alphabet, Inc.	2,45 – 2,65 mds
5	YouTube (US) Réseau social de partage de vidéos en streaming (<i>i.e.</i> en flux continu) et en direct Propriété d'Alphabet, Inc.	2,3 – 2,6 mds
6	WhatsApp (US) Réseau social vocal (VoIP), vidéo (appels vidéo et vidéoconférences) et de messagerie instantanée (messages textes) Propriété de Meta Platform	2,1 – 2,3 mds
7	GMail (US) Boîte de messagerie Propriété d'Alphabet, Inc.	1,8 – 2 mds
8	Instagram (US) Réseau social de partage de contenus Propriété de Meta Platform	1,5 – 1,7 mds
9	App Store (US) Magasin d'applications Propriété d'Apple, Inc.	1,4 – 1,6 md
10	Google Maps (US) Service de cartographie Propriété d'Alphabet, Inc.	1,35 – 1,55 md
11	iCloud (US) Application de stockage de fichiers en cloud Propriété d'Apple, Inc.	1,3 – 1,5 md
12	WeChat (CN) Réseau social vocal (VoIP), vidéo (appels vidéo et vidéoconférences) et de messagerie instantanée (texte) Propriété de Tencent Holdings Limited	1,3 – 1,4 md
13	iMessage (US) Réseau social de messagerie instantanée Propriété d'Apple, Inc.	1,3 – 1,35 md
14	Wikipedia (US) Wiki et encyclopédie en ligne Propriété de Wikimedia Foundation (organisme non lucratif)	1,1 – 1,3 md
15	TikTok / Douyin (CN) Réseau social de partage de courtes vidéos Propriété de ByteDance Ltd.	1,1 – 1,175 md
16	Google Translate (US) Service de traduction multilingue Propriété d'Alphabet, Inc.	975 millions – 1,15 md

17	Safari (US) Navigateur Web Propriété d'Apple, Inc.	975 millions – 1,075 md
18	Google Drive (US) Application de stockage de fichiers en cloud Propriété d'Alphabet, Inc.	950 millions – 1,05 md
19	Messenger (US) Réseau social de messagerie instantanée Propriété de Meta Platform	920 – 960 millions
20	TaoBao (CN) Service de commerce en ligne C2C (consommateur à consommateur, <i>i.e.</i> particulier à particulier) Propriété d'Alibaba Group	875 millions
21	Pornhub (LU) Application de partage de vidéos pornographiques Propriété de MindGeek	750 – 950 millions
22	Alipay (CN) Service de paiement en ligne Propriété d'Alibaba Group	815 – 845 millions
23	XVideos (CZ) Application de partage de vidéos pornographiques Propriété de WGCZ Holding	725 - 925 millions
24	Tmall (CN) Service de commerce en ligne B2C de produits haut de gamme Propriété d'Alibaba Group	780 millions
25	WeChat Pay (CN) Service de paiement en ligne Propriété de Tencent Holdings Limited	715-760 millions
26	Gaode Map / Autonavi Map (CN) Service de cartographie Propriété d'Alibaba Group	730 millions
27	Telegram (AE et UK) Réseau social de messagerie instantanée Propriété de Telegram Messenger Inc.	700 millions
28	Google Assistant (US) Assistant vocal intelligent Propriété d'Alphabet, Inc.	650 – 750 millions
29	Google Ads (US) Régie publicitaire Propriété d'Alphabet, Inc.	650-720 millions [d'internautes cliquant sur une publicité diffusée par Google Ads chaque mois]
30	Baidu Search (CN) Moteur de recherche Propriété de Baidu, Inc.	630 - 640 millions
31	Kuaishou (CN) Réseau social de partage de courtes vidéos, de courts extraits audios, de montage photo-vidéo et de messagerie instantanée Propriété de Kuaishou Technology	605-625 millions
32	PinDuoDuo (CN) Service de commerce en ligne C2M (consommateur à fabricant) de produits alimentaires agricoles Propriété de PinDuoDuo, Inc.	610-620 millions
33	Siri (US) Assistant vocal intelligent Propriété d'Apple, Inc.	550-625 millions

34	QQ (CN) Réseau social de messagerie instantanée et portail web Propriété de Tencent Holdings Limited	570 – 600 millions
35	Snapchat (US) Réseau social de partage de courtes vidéos, de courts extraits audios, de montage photo-vidéo et de messagerie instantanée Propriété de Snap Inc.	576 millions
36	Apple Maps (US) Service de cartographie Propriété d'Apple	480 – 665 millions
37	OneDrive (US) Application de stockage de fichiers en cloud Propriété de Microsoft Corporation	500 – 600 millions
	Yahoo! Search (US) Moteur de recherche et portail web Propriété de Yahoo, Inc.	
39	QQ Browser (CN) Navigateur web Propriété de Tencent Holdings Limited	510 – 545 millions
40	Rich Communication Service (US) Messagerie instantanée / SMS Propriété d'Alphabet	500 – 545 millions
41	Baidu Map (CN) Service de cartographie Propriété de Baidu, Inc.	521 millions
42	Alibaba / 1688.com (CN) Service de commerce en ligne B2B (professionnel à professionnel) et B2C (professionnel à consommateur) Propriété d'Alibaba Group	493 millions
43	Microsoft.com (US) Service d'offre logicielle, de conseil et d'assistance de Microsoft Propriété de Microsoft Corporation	490 millions
44	Spotify (SE) Service de distribution et de partage de musiques en streaming Propriété de Spotify Technology S.A	456 – 489 millions
45	JD (CN) Site de commerce en ligne B2C Propriété de Jingdong Mall	457 – 473 millions
46	Visa (US) Service de paiement en ligne Propriété de Visa, Inc.	425 – 500 millions
47	UC Browser (CN) Navigateur web Propriété d'Alibaba Group	435 – 475 millions
49	Sina Weibo (CN) Réseau social de microblog Propriété de Sina Corporation Corporation	445 – 460 millions
50	Pinterest (US) Réseau social de partage d'images Propriété de Pinterest Inc.	445 – 450 millions
51	Bitly (US) Service de réduction d'URL Propriété de Bitly, Inc.	436 millions

52	iQIYI (CN) Service de streaming de vidéos à la demande Propriété de Baidu, Inc.	415 – 465 millions
53	Reddit (US) Réseau social de partage de contenus dans des forums Propriété de Reddit Inc.	430 millions
54	The Weather Channel (US) Service de prévisions et d'analyses météo Propriété d'IBM	400 – 425 millions
55	Bing (US) Moteur de recherche et portail web Propriété de Microsoft	400-425 millions
56	Tencent Video (CN) Service de distribution de vidéos à la demande Propriété de Tencent Holdings Limited	405 – 425 millions
57	Twitter (US) Réseau social de microblog Propriété de Twitter Inc.	368 – 436 millions
58	Nhentai.net (IS) Service de lecture de hentai Propriétaire (?)	394 millions
59	Mi Store (CN) Magasin d'applications Propriété de Xiaomi Corporation	350 – 420 millions
60	Apple.com (US) Service d'offre logicielle, de conseil et d'assistance d'Apple Propriété d'Apple, Inc.	383 millions
61	TouTiao (CN) Réseau social de partage de contenus et agrégateur d'actualités Propriété de ByteDance Ltd.	350 - 380 millions
62	Aliexpress (CN) Service de commerce en ligne B2C Propriété d'Alibaba Group	373 millions
63	Meituan (CN) Application de livraison alimentaire Propriété de Meituan	350 – 385 millions
64	Fandom (US) Wiki tenu par et destiné aux fans Propriété de Fandom, Inc., filiale lucrative de Wikimedia Foundation	350-375 millions
	Opera (CN) Navigateur web Propriété du consortium Golden Brick Silk Road	
66	WiFi Master (CN) Service de partage WiFi en P2P (des utilisateurs partagent leur réseau WiFi pour permettre à d'autres de s'y connecter gratuitement) Propriété de LinkSecure	335 – 370 millions
67	Outlook (US) Boîte de messagerie (autrefois Hotmail) Propriété de Microsoft Corporation	347 millions

68	XNXX.com (CZ) Application de partage de vidéos pornographiques Propriété de WGCZ Holding	300 – 375 millions
	Union Pay (CN) Moyen de paiement en ligne Propriété totale de l'État chinois	315 – 360 millions
70	Kingsoft Documents (CN) Application de stockage de fichiers en cloud Propriété de Kingsoft Corporation	320 – 350 millions
71	AppGallery (CN) Magasin d'applications Propriété de Huawei	315 – 350 millions
72	Bilibili (CN) Réseau social de partage de vidéos en streaming Propriété de Bilibili, Inc.	332 millions
73	360 Game (CN) Plateforme de mini-jeux en ligne Propriété de Qihoo 360 Technology	315 – 345 millions
74	Xigua Video (CN) Réseau social de partage de courtes vidéos Propriété de ByteDance Ltd.	325 millions
	Baidu Knows / Baidu Zhidao (CN) Réseau social de questions-réponses Propriété de Baidu	300 – 350 millions
76	Alexa (US) Assistant vocal intelligent Propriété d'Amazon	300 – 345 millions
	OPPO Software Store (CN) Magasin d'applications Propriété de BBK Electronics Corporation	305 – 340 millions
78	XHamster (CY) Site web de partage de vidéos pornographiques Propriété de Hammy Media	285 – 350 millions
79	Alimama (CN) Régie publicitaire Propriété d'Alibaba Group	285 – 350 millions
80	KuGou (CN) Service de distribution et de partage de musiques en streaming Propriété de Tencent Holdings Limited	309 millions
81	Amazon (US) Service de commerce en ligne B2C (professionnel à consommateur) et C2C (consommateur à consommateur, <i>i.e.</i> particulier à particulier) Propriété d'Amazon	305 – 310 millions
82	Skype (US) Réseau social vocal (VoIP), vidéo (appels vidéo et vidéoconférences) et de messagerie instantanée (messages textes) Propriété de Microsoft Corporation	300 – 310 millions
	MX Taka Tak (IN) Réseau social de partage de courtes vidéos Propriété de Times Internet (en cours d'acquisition par Share Chat)	
84	Quora (US) Réseau social de questions-réponses Propriété de Quora, Inc.	275 – 310 millions

85	Mega.nz (NZ) Service d'hébergement de fichiers (ex-Megaupload) Propriété de Mega Limited	291 millions
86	MX Player (IN) Service de distribution de vidéos à la demande Propriété de Times Internet	290 millions
87	Mango TV (CN) Service de distribution de vidéos (émissions de télévision, séries, films, dessins animés) et de musiques à la demande Propriété de Hunan Broadcasting System (État chinois)	288 millions
88	Livejasmin.com (LU) Service de sexcam en direct Propriété de JWS America S.A.R.L.	282 millions
89	Accelerated Mobile Page (US) Projet open source (accessible, réutilisable et modifiable par tous) proposant un <i>framework</i> (code source qui forme le squelette d'un logiciel) conçu par Alphabet pour accélérer l'accès à des sites web Propriété d'Alphabet	281.5 millions
90	Mastercard (US) Moyen de paiement en ligne Propriété de Mastercard, Inc.	250 – 310 millions
	VIVO App Store (CN) Magasin d'applications Propriété de BBK Electronics	265 – 295 millions
92	Fifa.com Site web officiel de la Fédération internationale de football association (FIFA) Propriété de la FIFA	276 millions [en période de coupe du monde de football]
93	QQ Music (CN) Service de streaming musical Propriété de Tencent Holdings Limited	275 millions
	Microsoft Teams (US) Réseau social professionnel vocal (VoIP), vidéo (vidéoconférences) et de messagerie instantanée multimédias (textes, images, vidéo) par chats ou canaux de discussion réservés aux équipes de travail Propriété de Microsoft Corporation	270 – 280 millions
95	Mediafire.com (US) Service d'hébergement de fichiers Propriété de MediaFire, LLC	274 millions
96	QQ News (CN) Agrégateur d'actualités Propriété de Tencent Holdings Limited	250 – 290 millions
97	Fortnite (US) Jeu vidéo en ligne Propriété d'Epic Games	263 millions
98	Vimeo (US) Réseau social de partage de vidéos en streaming Propriété d'IAC (InterActiveCorp)	260 millions
99	Edge (US) Navigateur Web Propriété de Microsoft Corporation	225 – 285 millions
100	Youku (CN) Réseau social de partage de vidéos en streaming et en direct Propriété d'Alibaba Group	240 – 265 millions

101	Viber (JP) Réseau social vocal (VoIP), vidéo (appels vidéo), et de messagerie instantanée multimédias (texte, images, vidéos) Propriété de Rakuten Group, Inc.	250 millions
102	Rule34.xxx (?) Services d'hébergement d'images de hentai ou yaoi Propriétaire (?)	247.8 millions
103	Noodlemagazine.com (UA) Site web de partage de vidéos pornographiques Propriété de Vitaliy Root	246 millions
104	Apple Pay (US) Moyen de paiement en ligne Propriété d'Apple, Inc.	210 – 280 millions
105	NetEase Mail (CN) Boîte de messagerie Propriété de NetEase	244 millions
106	Candy Crush (UK) Jeu vidéo en ligne Propriété de King Digital Entertainment	240 millions
107	PUBG: Battlegrounds (CN) Jeu vidéo en ligne Copropriété de Tencent Holdings Limited	238 millions
108	Tencent Advertising (CN) Régie publicitaire Propriété de Tencent Holdings Limited	190 – 285 millions
	FaceTime (US) Réseau social vocal (VoIP) et vidéo (appels vidéos et vidéoconférences) Propriété d'Apple, Inc.	200 - 275 millions
110	Netflix (US) Service de distribution de vidéos à la demande Propriété de Netflix, Inc.	220 – 250 millions
111	Indeed (US) Moteur de recherche d'emploi Propriété de Recruit	230 millions
	Office.com (US) Site web de téléchargement d'une suite bureautique (Word, Excel, Powerpoint, OneNote, Outlook...) Propriété de Microsoft Corporation	
113	Youporn (LU) Service d'hébergement et de partage de vidéos pornographiques Propriété de MindGeek	228 millions
	Imgur (US) Réseau social d'hébergement et de partage d'images Propriété de Media Lab AI, Inc.	
115	Shazam (US) Service d'identification de musiques, films, publicités et émissions de télévision Propriété d'Apple, Inc.	225 millions
116	DingTalk (CN) Réseau social vocal (appels vocaux), vidéo (appels vidéos et vidéoconférence) et de messagerie instantanée Propriété d'Alibaba Group	224.7 millions

117	Chapmanganato.com (?) Service de lecture de mangas Propriétaire (?)	222 millions
118	Hanime.tv (US) Service d'hébergement de vidéos hentai Propriété de Registry Services, LLC	217 millions
119	Pixiv.net (JP) Réseau social communautaire dédié aux artistes Propriété de Pixiv, Inc.	216 millions
120	Meta Business Manager (US) Régie publicitaire Propriété de Meta Platform	200 – 230 millions
121	WordPress (US) Système de gestion de contenu Propriété de Automattic, Inc.	175 – 250 millions
122	UOL (BR) Moteur de recherche et portail web Propriété de Universo Online S.A.	212 millions
123	Animeflv.net (US) Portail de mangas animés Propriété de Domain Protection Services, Inc.	211 millions
124	Tencent MyApp (CN) Magasin d'applications Propriété de Tencent	160 – 260 millions
125	Roblox (US) Jeu vidéo en ligne Propriété de Roblox Corporation	204 millions
126	Tencent Cloud (CN) Application de stockage de fichiers en cloud Propriété de Tencent	190 – 215 millions
127	Healthline (US) Service de distribution d'informations médicales en ligne Propriété de Healthline Media, Inc.	201 millions
128	LinkedIn (US) Réseau social professionnel Propriété de Microsoft Corporation	200 millions
	Amazon Prime Video (US) Service de distribution de vidéos à la demande Propriété d'Amazon	
130	IMDb (US) Base de données sur le monde du cinéma, de la TV et des jeux vidéo Propriété d'Amazon	195 – 205 millions
131	Taboola (US) Service de fourniture de publicités (délivrant des publicités à d'autres applications qui les diffusent, par exemple via les recommandations) Propriété de Taboola, Inc.	199 millions
	BBC (UK) Journal d'actualités en ligne Propriété de la British Broadcasting Corporation	
133	CNN (US) Journal d'actualités en ligne Propriété de CNN News Group	198 millions
134	Samsung.com (KR) Service d'information, de conseil et d'offre de produits Samsung Propriété de Samsung Group	197 millions

135	Booking (NL) Service de réservation de logements Propriété de Booking Holdings	195,5 millions
136	MSN (US) Portail web et agrégateur d'actualités Propriété de Microsoft Corporation	195,2 millions
137	Yahoo! Mail (US) Boîte de messagerie Propriété de Yahoo, Inc.	175 – 215 millions
138	Paypal (US) Service de paiement en ligne Propriété de Paypal Holdings, Inc.	170 – 220 millions
	Apple Watch (US) Montre connectée Propriété d'Apple Inc.	175 – 215 millions
	JD Pay (CN) Moyen de paiement en ligne Propriété de Jingdong Mall	185 – 205 millions
141	Tnaflix.com (?) Site de distribution de vidéos pornographiques Propriétaire (?)	194.8 millions
142	DuckDuckGo (US) Moteur de recherche Propriété de Duck Duck Go, Inc.	193 millions
143	VIVO Game Center (CN) Application de téléchargement, de gestion et d'organisation de jeux vidéo téléchargés sur mobile Propriété de BBK Electronics Corporation	180-200 millions
144	Naver (KR) Moteur de recherche et portail web Propriété de Naver Corporation	189.8 millions
145	Redtube (LU) Site web de partage de vidéos pornographiques Propriété de MindGeek	188.7 millions
146	Linktree (AU) Service de pages de renvoi vers des annonces publicitaires depuis des réseaux sociaux Propriété de Bolster Creative Pty Ltd	188.1 millions
147	Disney Plus (US) Service de distribution de vidéos à la demande Propriété de The Walt Disney Company	185 - 190 millions
148	Thepornbude.com (US) Portail d'accès à des sites pornographiques Propriétaire (?)	185.5 millions
149	Line (JP) Réseau social vocal (VoIP), vidéo (appels vidéos et vidéoconférences) et de messagerie instantanée (texte) Propriété de Line Corporation	185 millions
	Gaana (IN) Application de distribution de musiques et de partage de playlists entre utilisateurs Propriété de Times Internet	

151	Eporner.com (US) Application de partage de vidéos pornographiques Propriétaire (?)	184 millions
152	The New York Times (US) Journal d'actualités en ligne Propriété de The New York Times Company	183.5 millions
153	Share Chat (IN) Réseau social de partage d'images et de vidéos, de messagerie instantanée, de salles de discussion audio, de microblog et de blogs Propriété de Mohalla Tech Pvt Ltd. (Share Chat)	180 – 185 millions
154	NetEase Cloud Music (CN) Application de distribution de musiques en streaming (<i>i.e.</i> en flux continu) Propriété de NetEase	181.7 millions
155	Mi Game Center (CN) Application de téléchargement, de gestion et d'organisation de jeux vidéo téléchargés sur mobile Propriété de Xiaomi Corporation	170 – 190 millions
	Mozilla Firefox (US) Navigateur web Propriété de Mozilla Foundation	165 – 195 millions
157	Adobe.com (US) Site web d'information, de conseil et d'offre de produits Adobe Propriété d'Adobe, Inc.	179 millions
158	Yelp (US) Réseau social d'hébergement d'avis participatifs sur des entreprises Propriété de Yelp, Inc.	178 millions
159	Dailymotion (FR) Réseau social de streaming vidéo Propriété de Vivendi	177 millions
160	Sound Cloud (DE) Application de distribution de fichiers audios et de partage de musiques Propriété de SoundCloud Ltd	175,5 millions
161	Mi Video (CN) Réseau social de partage de vidéos en streaming Propriété de Xiaomi Corporation	160 – 190 millions
	58.com (CN) Plateforme d'hébergement de petites annonces Propriété de 58.com, Inc.	175 millions
163	Minecraft (US) Jeu vidéo en ligne Propriété de Microsoft Corporation	172,8 millions
164	Moji Weather (CN) Service de prévisions et d'analyse météo Propriété de Moji Co. Ltd.	165 – 180 millions
165	Pornzog.com (IS) Agrégateur de vidéos pornographiques publiées sur des sites pornographiques tiers Propriétaire (?)	171,6 millions

166	Onlyfans (UK) Service d'abonnement souscrit par des fans pour accéder au contenu (souvent sexuel) du créateur de contenus Propriété de Fenix International Limited	170 millions
	Moj (IN) Réseau social de partage de courtes vidéos Propriété de Mohalla Tech Pvt Ltd. (ShareChat)	160 - 180 millions
168	Hitomi.la (?) Service d'hébergement d'images hentai Propriétaire (?)	169,2 millions
169	Outbrain (US) Service de fourniture de publicités Propriété d'Outbrain, Inc.	169,1 millions
170	Steam (US) Plateforme de vente en ligne de jeux vidéo et de discussion entre communautés de joueurs Propriété de Valve Corporation	167,9 millions
171	Discord (US) Réseau social vocal (VoIP), vidéo (appels vidéo) et de messagerie instantanée par chat privés ou communautés Propriété de Discord, Inc.	160 – 190 millions
172	PhonePe (IN) Service de paiement en ligne Propriété de PhonePe Pvt Ltd	150 – 185 millions
	Tenpay (CN) Service de paiement en ligne Propriété de Tencent Holdings Limited	160 – 175 millions
174	Google Pay (US) Service de paiement en ligne Propriété d'Alphabet, Inc.	155 – 170 millions
	Baidu Baike (CN) Wiki / Encyclopédie en ligne Propriété de Baidu	150 – 175 millions
176	Chaturbate.com (US) Service de sexcam en direct Propriétaire (?)	160 millions
	Twitch (US) Réseau social de partage de vidéos en direct Propriété d'Amazon	145 – 175 millions
178	Little Red Book ou RED / Xiaohongshu (CN) Réseau social de partage d'avis sur des produits Propriété de Xingin Information Technology (Shangai) Co. Ltd	158 millions
179	Stripchat.com (IS) Service de sexcam en direct Propriétaire (?)	157 millions
180	Erome.com (US) Site web de partage de vidéos pornographiques Propriétaire (?)	155 millions
181	King of Glory (CN) Jeu vidéo en ligne Propriété de Tencent	154 millions
182	Josh (IN) Réseau social de courtes vidéos Propriété de VerSe Innovation Pvt. Ltd.	153 millions

183	Cortana (US) Assistant vocal intelligent Propriété de Microsoft Corporation	145 – 160 millions
184	Waze (US) Service de cartographie Propriété d'Alphabet, Inc.	151 millions
185	Fc2.com (CA) Portail web Propriétaire (?)	150 millions
	Kuwo (CN) Application de distribution de musiques en streaming Propriété de Tencent Holdings Limited	
	Central Brasileira de Notícias (BR) Journal d'actualités en ligne Propriété de Grupo Globo	
	Likee (SG) Réseau social de partage de courtes vidéos Propriété de JOYY Inc.	
	Dailyhunt (IN) Agrégateur d'actualités Propriété de VerSe Innovation Pvt. Ltd.	140 – 160 millions
	Google News (US) Agrégateur d'actualités Propriété d'Alphabet, Inc.	
	YouTube Ads (US) Régie publicitaire Propriété d'Alphabet, Inc.	115 – 185 millions
192	League of Legends (US) Jeu vidéo en ligne Propriété de Riot Games, filiale de Tencent Holdings Limited	148.5 millions
193	DouYu (CN) Réseau social de partage de vidéos en direct Propriété de DouYu International Holdings Ltd.	130 – 165 millions
194	Tumblr (US) Réseau social de microblog Propriété de Automattic, Inc.	147 millions
195	Anipop (CN) Jeu en ligne Propriété de Happy Elements Technology	130 – 160 millions
196	Txxx.com (IS) Site web de partage de vidéos pornographiques Propriétaire (?)	144.5 millions
	Lectortmo.com (ES) Site web de lecture de mangas Propriétaire (?)	
198	Meitu Pic / Meitu XiuXiu (CN) Service de montages photo Propriété de Meitu Inc.	141 millions
199	Mayoclinic (US) Service clinique d'information, de conseil et de prise de rendez-vous médicaux Propriété de Mayo Foundation for Medical Education and Research	140.6 millions
200	Bet365 (UK) Service de jeu de hasard en ligne (paris sportifs, jeux de casino...) Propriété de Bet365 Group Ltd.	140.4 millions

201	Sogou (CN) Moteur de recherche Propriété de Sohu, filiale de Tencent	135 – 145 millions
202	ByteDance Advertising (CN) Régie publicitaire Propriété de ByteDance Ltd.	100 – 175 millions
	Sina News (CN) Agrégateur d'actualités Propriété de Sina Corporation	125 – 155 millions
204	NetEase News (CN) Agrégateur d'actualités Propriété de Netease	120 – 150 millions
205	Ebay (US) Service de commerce en ligne B2C et C2C Propriété de eBay, Inc.	130 – 140 millions
206	Fapello.com (BS) Site web de partage d'images érotiques et pornographiques Propriétaire (?)	134.5 millions
207	Medium (US) Service de journalisme amateur, d'hébergement de blogs et de publications d'articles Propriété de A Medium Corporation	130.9 millions
208	Among Us (US) Jeu vidéo mobile en ligne Propriété de InnerSloth LLC	100 – 160 millions
	Huawei Mobile Cloud (CN) Application de stockage de fichiers en cloud Propriété de Huawei	90 – 170 millions
210	Canva (AU) Plateforme de conception graphique et de partage sur les réseaux sociaux Propriété de Canva Pty SA	128,5 millions
211	Missav.com (CH) Site web de distribution de vidéos pornographiques Propriétaire (?)	128 millions
212	IGN (US) Application d'actualités et de critiques sur les jeux vidéo Propriété d'IGN Entertainment, Inc.	127.8 millions
213	The Guardian (UK) Journal d'actualités en ligne Propriété de Guardian Media Group plc	125 millions
	USPS (US) Service postal fédéral des États-Unis Propriété du United States Postmaster General (État)	
	Meesho (IN) Service de commerce en ligne B2C de produits mis en vente par des commerçants désireux de faire connaître leur entreprise en ligne Propriété de Fashnear Technologies Private Limited	
	Apple News (US) Agrégateur d'actualités Propriété d'Apple, Inc.	
	DoubleClick / Google Marketing Platform (US) Régie publicitaire Propriété d'Alphabet, Inc.	80 – 170 millions

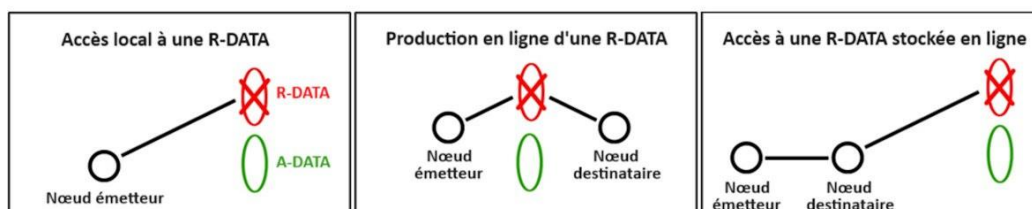
218	Walmart (US) Service de commerce en ligne B2C Propriété de Walmart Inc.	118 – 125 millions
219	AccuWeather (US) Service de prévisions et d'analyses météo Propriété d'AccuWeather, Inc.	120,5 millions
220	Youdao Dictionary (CN) Service de traduction multilingue Propriété de NetEase	120 millions
	BestPay (CN) Service de paiement en ligne Propriété de China Telecom (État)	115 – 125 millions
	Xianyu (CN) Service de commerce en ligne Propriété d'Alibaba Group	
223	E-hentai.org (US) Site de partage et d'hébergement d'images hentai Propriétaire (?)	116.6 millions
224	Zillow (US) Moteur de recherche d'annonces immobilières Propriété de Zillow Group, Inc.	115.5 millions
225	Mi AI (CN) Assistant vocal intelligent Propriété de Xiaomi Corporation	105 – 125 millions
226	WebMD (US) Service de distribution d'informations médicales et d'hébergement de blogs de médecins Propriété de Internet Brands, Inc.	114.8 millions
227	Momo (CN) Application de rencontre Propriété de Momo, Inc.	114 millions
	Directcpmrev.com (US) (site suspect) Site web non sécurisé de renvoi vers des annonces publicitaires et des sites web suspects voire infectés par des logiciels malveillants Propriétaire (?)	
229	Apex Legends (US) Jeu vidéo en ligne Propriété d'Electronic Arts, Inc. (EA)	113 millions
230	9anime (VN) Portail d'accès à des mangas animés en streaming Propriété de Tran Ngoc Chinh	105 – 120 millions
	Capcut (CN) Application de montage vidéo Propriété de ByteDance Ltd.	100 – 125 millions
232	Genius (US) Service de publication et d'hébergement de textes (paroles de chansons, scripts cinématographiques ou télévisuels, écrits et discours historiques...) annotés par les utilisateurs Propriété de Genius Media Group, Inc.	111 millions

233	WeCom / WeChat Work (CN) Application de gestion des données d'entreprise, et réseau social professionnel vidéo (vidéokonférences) et de messagerie instantanée (texte, images, vidéos) pour communiquer avec les partenaires, employés, collègues et consommateurs Propriété de Tencent Holdings Limited	110,8 millions
234	Haokan Video (CN) Réseau social de courtes vidéos Propriété de Baidu, Inc.	100 – 120 millions
	Tmall Genie (CN) Assistant vocal intelligent Propriété d'Alibaba Group	90 – 130 millions
236	Fanqie Novel (CN) Application de lecture, d'écoute et de gestion des livres électroniques, et réseau social de partage d'avis des lecteurs Propriété de ByteDance Ltd.	109 millions
237	Internet Archive / Archive.org (US) Bibliothèque numérique et archivage du Web Propriété d'Internet Archive (organisme à but non lucratif)	108 millions
238	HBO Max (US) Service de distribution de vidéos à la demande Propriété de Warner Bros. Discovery, Inc.	105-110 millions
239	QQ Mail (CN) Boîte de messagerie Propriété de Tencent Holdings Limited	95 – 120 millions
240	WikiHow (US) Wiki de publication de guides pratiques Propriété de WikiHow, Inc.	107.1 millions
	Wiktionary (US) Wiki / Dictionnaire en ligne Propriété de Wikimedia Foundation	
242	Youjizz.com (LU) Site web de partage de vidéos pornographiques Propriétaire (?)	107 millions
243	Manganato.com (US) Service de lecture de mangas en ligne Propriétaire (?)	105.5 millions
244	Tencent WiFi Manager (CN) Service de connexion à des points Wi-Fi fournis par Tencent Propriété de Tencent Holdings Limited	100-110 millions
245	Baidu Wangpan (CN) Application de stockage de fichiers en cloud Propriété de Baidu, Inc.	104.5 millions
246	JioSaavn (IN) Service de distribution de musiques en streaming Propriété de Saavn Media Pvt. Ltd.	104 millions
247	JustWatch (DE) Portail d'accès à des vidéos à la demande Propriété de JustWatch GmbH	103.2 millions
248	Gamespot.com (US) Site web d'actualités et d'analyses de jeux vidéo Propriété de Fandom, Inc., filiale lucrative de Wikimedia Foundation	103.1 millions

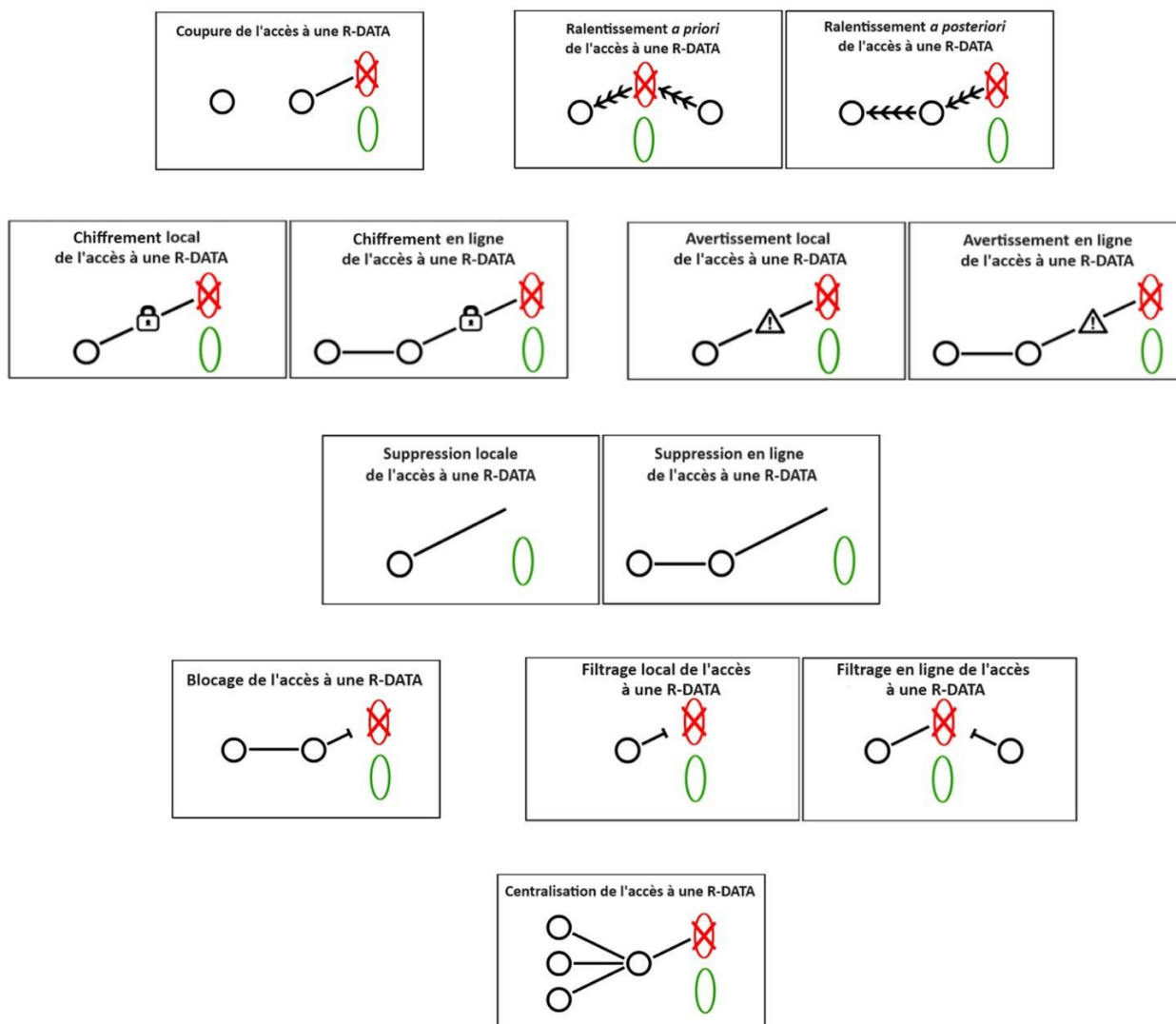
249	Zhihu (CN) Réseau social de questions-réponses Propriété de Zhihu, Inc.	100 - 105 millions
	Sina Tianqitong (CN) Service de prévisions et d'analyses météo Propriété de Sina Corporation	95 – 110 millions
251	Vkontakte / VK (RU) Réseau social de partage de contenus Propriété de Mail.ru	101,7 millions
252	Redgifs.com (US) Site web de partage d'images et de vidéos pornographiques Propriétaire (?)	101,3 millions
253	Stack Exchange (US) Réseau social de questions-réponses Propriété de Stack Exchange, Inc.	101 millions
254	DMM.com (JP) Service de commerce en ligne B2C, de location de biens et services, d'accès à des jeux vidéo en ligne et de distribution de vidéos à la demande Propriété de DMM.com LLC	100,9 millions
255	Dropbox (US) Application de stockage de fichiers en cloud Propriété de Dropbox Inc.	75 – 125 millions
	Yandex (RU) Moteur de recherche et portail web Propriété de Yandex LLC	85 – 115 millions
	Zoom (US) Service de vidéoconférence Propriété de Zoom Video Communications	
258	Yahoo News (US) Agrégateur d'actualités Propriété de Yahoo, Inc.	78 – 120 millions
259	Baidu Advertising (CN) Régie publicitaire Propriété de Baidu, Inc.	70 – 125 millions
	DuerOS / Xiaodu Assistant (CN) Assistant vocal intelligent Propriété de Baidu, Inc.	80 – 115 millions
261	Google AdSense (US) Régie publicitaire Propriété d'Alphabet, Inc.	50 – 135 millions
262	Amazon Ads (US) Régie publicitaire Propriété d'Amazon	75 - 100 millions
263	Celia (CN) Assistant vocal intelligent Propriété de Huawei	60 – 100 millions
264	Microsoft Advertising (US) Régie publicitaire Propriété de Microsoft Corporation	45 – 100 millions

Annexe 2. Synthèse des configurations expérimentées dans la thèse

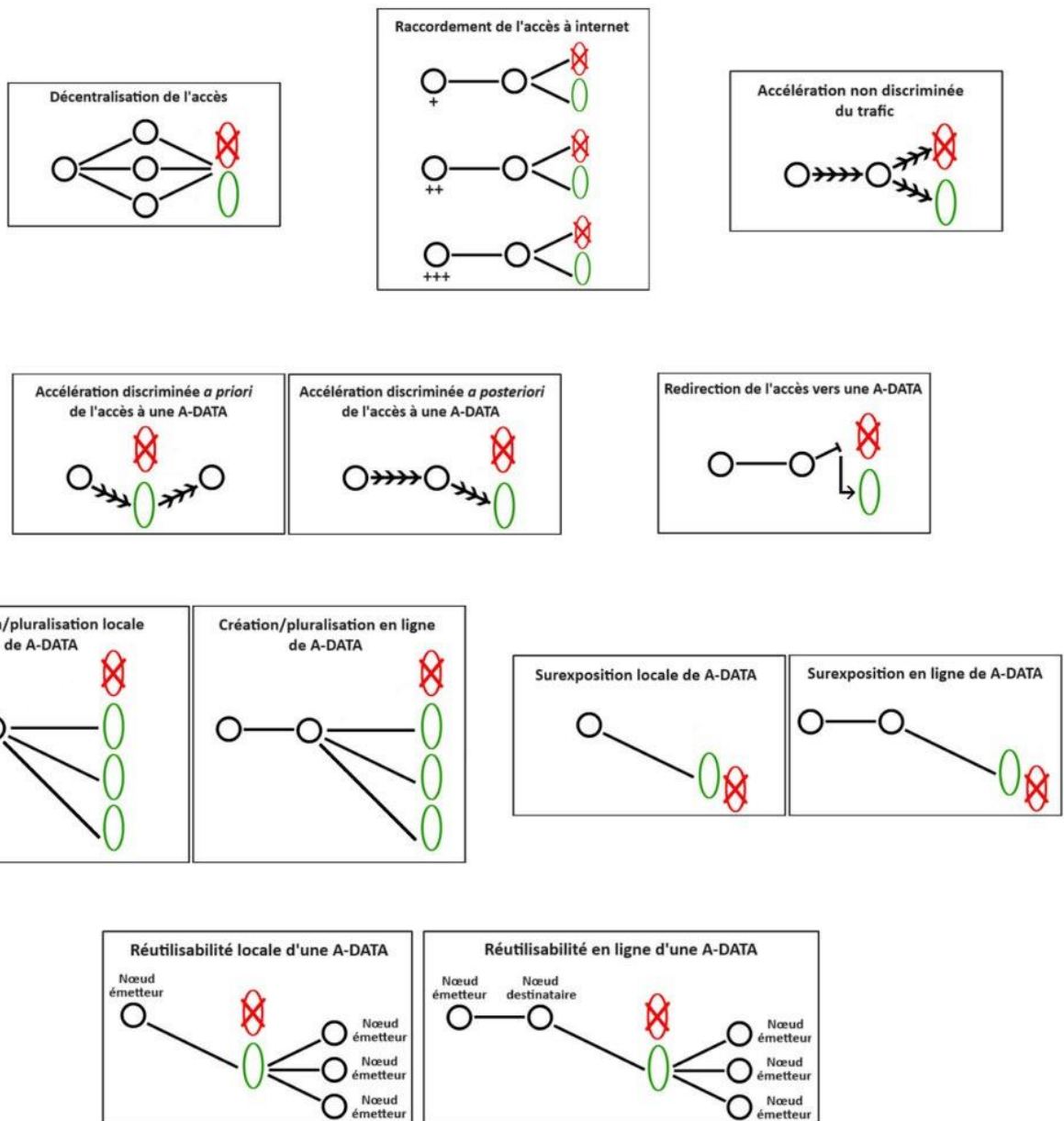
Configurations d'accès à une R-DATA



Techniques de restriction de l'accès échantillonnées dans la thèse



Techniques d'augmentation de l'accès échantillonnées dans la thèse



Configurations identifiées de contournement d'une restriction d'accès

