

Influence de la culture sur les réponses face à une violation de données personnelles

Thèse de Doctorat présentée en vue de l'obtention
du grade de docteur en sciences de gestion et du Management
par

Christelle AUBERT HASSOUNI

dirigée par

Mme Sandrine MACE, Professeure – ESCP Business School
Mme Béatrice PARGUEL, Directrice de recherche – CNRS, PSL, DRM

Soutenance le 13 avril 2023

Devant un jury composé de :

Rapporteurs :

Mme Caroline LANCELOT MILTGEN
Professeure – Audencia Business School
M. Pierre VALETTE FLORENCE
Professeur – Université Grenoble Alpes

Suffragants :

Mme Cécile CHAMARET
Professeure – École Polytechnique
M. Yany GREGOIRE
Professeur – HEC Montréal

L'Université n'entend donner aucune approbation ni improbation
aux opinions émises dans cette thèse :
ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Alors que cette très belle aventure académique va bientôt prendre fin, je suis heureuse de pouvoir remercier toutes les personnes sans lesquelles elle n'aurait pas pu être possible.

Ma plus sincère gratitude revient à mes directrices de thèse, Sandrine Macé et Béatrice Parguel. Au-delà de leurs multiples conseils formulés, et constitutifs de cette recherche, au-delà leur soutien sans faille, très grande disponibilité, de leur patience et compréhension face aux aléas de ma quête, de mes tâtonnements et multiples projets, elles resteront pour moi de vraies guides. J'espère savoir faire preuve à l'avenir d'autant de justesse, de bon sens, de simplicité, de peps et de bonne humeur. À leurs côtés, j'ai vécu une aventure tout autant humaine qu'intellectuelle : elles peuvent à leur tour compter sur moi à tout moment.

Je souhaite remercier chaleureusement les professeurs Caroline Lancelot Miltgen et Pierre Valette Florence, qui me font l'honneur d'être mes rapporteurs, et dont les nombreuses recommandations formulées lors de la pré-soutenance ont solidifié ce travail. Je remercie également les professeurs Cécile Chamaret et Yany Grégoire, d'avoir accepté de participer au jury et d'évaluer mon travail. La présence de chacun dans ce jury revêt à mes yeux un caractère symbolique des diverses facettes de ce travail de recherche.

J'ai eu la chance au cours de ce parcours académique d'être soutenue et conseillée par de nombreuses personnes. Je tiens à remercier Julien Cloarec : à travers nos très nombreuses collaborations, nos échanges m'ont permis d'avancer vite et de m'émanciper, un très grand merci pour cela ! J'adresse mes plus sincères remerciements à l'équipe du CEFAG et à la FNEGE, et particulièrement à Hervé Laroche et Géraldine Schmidt : nos séminaires et leur soutien ont été la bouffée d'oxygène de cette thèse en plein cœur de la crise sanitaire. Je souhaite également remercier l'ESCP Business School, dont plusieurs professeurs : Claire Dambrin, Hervé Laroche (bis repetita), Régis Coeurderoy, et au sein de l'équipe marketing, Olivier Badot, Michael Haenlein, Julien Schmitt, avec une pensée émue pour Raphaëlle Pandraud. Je remercie également Jean-François Lemoine et l'école doctorale Panthéon-Sorbonne. Mes remerciements vont également à Philippe Monin et Margherita Pagani, ainsi qu'à l'emlyon pour son soutien lors de la première partie de cette thèse. J'ai une reconnaissance toute particulière pour mes anciens collègues et amis Benjamin Huybrechts et Imène Brigui. Enfin je remercie Sarah Lasri et l'université Paris Dauphine-PSL. Je tiens à témoigner ma reconnaissance aux nombreuses

personnes (inconnues) qui ont relu mes communications et dont les commentaires et conseils m'ont été précieux, ainsi qu'à celles avec lesquelles j'ai pu échanger lors de colloques doctoraux et conférences. Ce parcours n'aurait pas été le même sans l'aide efficace et amicale de Christine Rocque, que je remercie chaleureusement. Enfin j'ai une pensée particulière pour Laurent Battais, qui m'a vu naître professionnellement et qui continue à être présent.

Une aventure de thèse est avant tout collective, et je remercie toutes et tous les jeunes chercheurs avec lesquels je l'ai partagée. En premier lieu, bien sûr, toute l'équipe des ateliers de Thésée : Lucie Cortambert, Lucie Denis, Fabienne Perez, Sandra Renou, Margaux Vales, et avant elles, Anne-Sophie Barbe, Fabien Canolle et Julien Cloarec (bis repetita). Également Chloé Steux, Camille Toussaint, Michelle Van Weere, Romain Debru et toute la promo CEFAG 2020 (malheureusement aussi appelée « promo Covid »). Mais aussi les doctorants de l'ESCP Business School, et tout particulièrement, Jannsen Santana, Aude Montlahuc, Yaëlle Amsallem, Sophie Gourevitch, Louis Vuarin, Thomas Simon (et ses Oasiens), et Nawel Dehiri. Pour finir, merci à Alex Deslee, Charlotte Cadieu, à l'équipe Juliette Senn, Hugo Gaillard, Albane Grandazzi, ainsi qu'à Delphine Godefroit-Winkel, Amélie Abadie, Sarah Belghiti.

Dans un registre plus personnel, mes premiers remerciements vont à Marine et Julien, sponsors sous toutes formes de cette thèse, ainsi qu'à Raphaële, pour avoir lu et relu ce manuscrit. Ma profonde affection revient à mes amis dont le soutien ont été mon carburant pour avancer : Virg et Seb, Olivier, Julie, Tonton K et Soussou, Yacout et Marco, Yas, Nono et Reda, et tous les autres ! Et merci aussi à Lagertha, Brigitta et Haloua.

À mes enfants, Mia et Malik, qui malgré les sacrifices familiaux que la réalisation de cette thèse a demandés ont toujours mesuré l'intérêt et la valeur de ce travail : cette attitude vous honore ! À Hicham, qui m'a donné l'envie, le courage et la force de réaliser cette recherche, qui l'a soutenue mentalement et matériellement à tous les instants et sans faiblir malgré les embûches, grâce à qui le plus compliqué devient simple en un instant, avec qui je continue à regarder loin devant, forts maintenant de cette tâche accomplie : l'aventure continue ! Show must go on !

À Mia et Malik,
puisse ce long travail vous donner des ailes.

« Le monde existe à travers nos sens avant d'exister de façon ordonnée dans notre pensée
et il nous faut tout faire pour conserver au fil de l'existence cette faculté créatrice de sens :
voir, écouter, observer, entendre, toucher, caresser, sentir, humer, goûter,
avoir du « goût » pour tout, pour les autres, pour la vie. »

Françoise Hériter, *Le sel de la vie*.

Sommaire

Introduction générale	1
Chapitre 1. Contexte général de la recherche	18
Section 1. Contexte managérial de la recherche.....	19
1. Violations de données personnelles : le « far-west »	19
2. Réglementations pour la protection des données personnelles.....	35
Section 2. Contexte académique de la recherche.....	51
1. Causes et effets des violations de données personnelles	51
2. Culture et souci de contrôle des données personnelles	61
Section 3. Axes de recherche et contributions attendues	78
Chapitre 2. Fondements théoriques	86
Section 1. Protection des données personnelles	87
1. Conceptualisation de la protection de la vie privée	87
2. Psychologie de la préoccupation pour la protection de la vie privée.....	101
3. Autres facteurs influençant les comportements de protection des données.....	109
Section 2. Réponses des consommateurs insatisfaits.....	113
1. Comportement de plainte du consommateur	114
2. Réponses pour la protection de la vie privée	121
Section 3. Culture et valeurs culturelles.....	126
1. Définition du concept de culture.....	127
2. Définition et compréhension des valeurs culturelles	135
3. Théories et structures de modèles de valeurs culturelles	140
Chapitre 3. Cadre général de la thèse	158
Section 1. Questions de recherche et cadre théorique général.....	159
1. Synthèse du contexte et des fondements théoriques	159
2. Trois niveaux d'observation : macro, méso et micro.....	161
3. Modèle conceptuel.....	166
Section 2. Positionnement épistémologique et méthodologies de recherche	167
1. Différence entre positivisme et interprétativisme	167
2. Approche post-positiviste	168
3. Méthodologies de recherche	171
Section 3. Structure de la thèse et apports de chaque essai.....	173
1. Description et objectifs de chaque essai	173
2. Apports de chaque essai à la thèse.....	175
3. Contributions des auteurs et stade d'avancement dans la publication des essais ..	177

Chapitre 4. Essai 1 - Influence de la culture nationale.....	182
Section 1. Introduction et fondements de la recherche.....	183
1. Introduction.....	183
2. Fondements théoriques	186
3. Étude exploratoire de la culture nationale en Europe	191
Section 2. Modèle conceptuel et hypothèses de recherche	193
1. Individualisme et plainte pour protection des données personnelles.....	193
2. Masculinité et plainte pour protection des données personnelles.....	194
3. Orientation à long terme et plainte pour protection des données personnelles.....	195
Section 3. Recherche empirique et résultats	197
1. Méthodologie	197
2. Première étape de l'analyse	199
3. Deuxième étape de l'analyse	200
Section 4. Discussion et implications.....	202
1. Contributions théoriques.....	202
2. Implications pratiques.....	203
3. Limites et voies de recherches	206
Chapitre 5. Essai 2 - Influence des normes socio-culturelles	212
Section 1. Introduction.....	213
Section 2. Fondements théoriques de la recherche.....	218
1. Valeurs et motivations socio-culturelles.....	218
2. Réponses engagées pour la protection des données personnelles.....	219
3. Théorie de la pratique	221
4. Facteurs influençant les réponses pour la protection de la vie privée.....	226
Section 3. Méthodologie et recherche empirique.....	231
1. Approche qualitative	232
2. Procédure de recrutement	232
3. Procédure d'entretiens	236
4. Méthode d'analyse.....	238
Section 4. Résultats descriptifs de la recherche	246
1. Actions de protection de la vie privée.....	246
2. Conséquences et valeurs culturelles identifiées	260
Section 5. Résultats analytiques de la recherche	263
1. Motivations socio-culturelles dominantes	263
2. Pratiques sociales de protection de la vie privée	271
Section 6. Discussion et implications.....	282
1. Contributions théoriques.....	283
2. Implications pratiques.....	286
3. Limites et voies de recherches	286

Chapitre 6. Essai 3 - Influence des orientations culturelles individuelles.. 290

Section 1. Introduction et fondements de la recherche.....	291
1. Introduction.....	291
2. Fondements théoriques	295
Section 2. Modèle conceptuel et développement des hypothèses.....	308
1. Distance psychologique et préoccupation pour la protection de la vie privée.....	308
2. Influence des orientations culturelles individuelles	310
3. Réponses face à une violation de données personnelles	318
Section 3. Recherche empirique et résultats	320
1. Méthodologie	320
2. Résultats.....	327
Section 4. Discussion et implications.....	333
1. Contributions théoriques	334
2. Implications pratiques	335
3. Limites et voies de recherche.....	337

Chapitre 7. Discussion et conclusion 342

Section 1. Contributions théoriques.....	344
1. Effets culturels sur les réponses aux violations de données personnelles	346
2. Réponses aux violations de données personnelles.....	349
3. Distance psychologique avec la protection de la vie privée	351
4. Théorie de la pratique et pratiques de protection de la vie privée	353
5. Nouvelle compréhension du souci de protection de la vie privée	356
Section 2. Implications pratiques	362
1. Développement de pratiques de protection de la vie privée	363
2. Discours médiatique et publicitaire	372
3. Évolutions réglementaires	377
Section 3. Limites et voies de recherche	380
1. Protection des données personnelles et de la vie privée	380
2. Réponses apportées aux violations de données personnelles	383
3. Culture et souci de protection de la vie privée.....	386

Conclusion générale 389

Liste des tableaux 393

Liste des figures..... 395

Tables des annexes 397

Tables des matières 398

Références bibliographiques 405

Annexes 426

Résumé de la thèse

Face à une explosion du nombre de violations de données personnelles (i.e., des vols intentionnels d'informations confidentielles touchant des individus dans un objectif lucratif), les réponses des individus, comme les plaintes auprès des régulateurs (e.g., CNIL), varient fortement entre pays. Ceci nous amène à interroger l'influence de possibles effets culturels dans les réponses face à une violation de données personnelles. Dans cette perspective, les recherches en cours, qui explorent principalement le lien entre préférence culturelle pour l'individualisme (i.e., défense de ses propres objectifs) et souci de protection de sa vie privée, appellent à faire varier les explorations pour éclairer les phénomènes.

Dans cette thèse, nous soutenons qu'une préférence culturelle pour des valeurs d'égalité sociale et de genre amène les individus à adopter des réponses plus actives face à une violation de leurs données personnelles. Nous montrons que cette préférence opère à trois niveaux d'observation : macro (institutionnel), méso (social), micro (psychologique).

- Premièrement, et à l'aide d'une base de données recensant des plaintes déposées auprès des régulateurs européens, nous observons que les individus vivant dans des pays valorisant davantage l'égalité des genres ont tendance à se plaindre davantage ;
- Deuxièmement, une recherche plus exploratoire (15 entretiens) montre que la défense de l'égalité sociale est une motivation essentielle à l'adoption d'une réponse active face à une violation. Et elle envisage la protection de la vie privée comme une pratique sociale (Bourdieu, 1972; Giddens, 1984), et non individuelle ;
- Troisièmement, une enquête (N=452) confirme les premiers résultats et affirme que l'égalité sociale et de genre sont les valeurs culturelles qui influencent le plus les réponses, impliquant moins de distance psychologique (Trope & Liberman, 2010) avec la violation de données personnelles.

Cette mise en lumière apporte une compréhension différente de la préoccupation pour la protection de la vie privée, envisagée comme un « mieux vivre ensemble » et non un « mieux vivre tout seul » et comme un souci de sécuriser les données personnelles de tous. Cet éclairage permet aussi d'enrichir la compréhension théorique des réponses aux violations de données personnelles et de leurs mécanismes : la protection de la vie privée est comprise comme une pratique sociale, et non individuelle, responsabilisant chaque acteur. Ainsi, des possibilités d'actions sont proposées aux politiques publiques et aux acteurs de la cybersécurité.

Introduction générale

Fin août 2022, les systèmes informatiques de l'hôpital de Corbeil-Essonnes sont bloqués par des pirates, réclamant une rançon de 10 millions de dollars en échange de la remise en fonctionnement des systèmes¹. La rançon n'est pas payée, conformément aux recommandations de l'ANSI². Après un mois de blocage, les pirates divulguent de nombreuses données médicales (e.g., examens de coloscopie ou de cancers du sein). Le centre hospitalier invite les patients (sûrement inquiets par la diffusion de leurs informations sensibles) et le personnel de santé (épuisé après un mois d'exercice médical sous contraintes) à porter plainte individuellement auprès de la CNIL (Commission Nationale Informatique et Libertés). Nous nous interrogeons alors sur leurs volonté et capacité individuelles à porter plainte dans ces circonstances. En particulier, la protection de la vie privée, droit individuel, peut-elle être appliquée sans moyen d'action plus collectif ?

En parallèle, de nombreuses réglementations de protection de la vie privée et des données personnelles sont établies à l'international (e.g., Règlement Général sur la Protection des Données – RGPD – en Europe), permettant de renforcer les possibilités de recours au droit, notamment par la saisine des régulateurs (e.g., CNIL en France). Cependant, le nombre de plaintes varie fortement entre les pays, notamment européens³, et est inversement proportionnel au montant des pénalités appliquées par les régulateurs (e.g., l'Espagne a imposé un montant total de sanctions depuis mai 2018 de près de 85 millions d'euros, contre un peu plus de 1,2 million d'euros pour le Danemark). Les lois sur la protection des données s'appliqueront d'ici 2024 à 75 % des consommateurs dans le monde⁴, soulignant la nécessité de leur convergence internationale face aux grandes questions commerciales mondiales (e.g., transferts de données entre l'Europe et les États-Unis suite à l'invalidation du Privacy Shields).

¹ Le Monde, 26.09.2022, disponible à : https://www.lemonde.fr/pixels/article/2022/09/26/apres-la-cyberattaque-contre-l-hopital-de-corbeil-essonnes-ce-que-l-on-sait-sur-les-donnees-diffusees_6143245_4408996.html et France Info, 9.10.2022 : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-a-l-hopital-de-corbeil-essonnes-patients-et-membres-du-personnel-incites-a-porter-plainte_5407198.html

² Cf. p.29 du rapport ANSSI (Agence Nationale de la Sécurité des Systèmes Informatiques) de septembre 2020 : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_ranconciels_tous_concernes-v1.0.pdf

³ DLA Piper GDPR fines and data breach survey. Disponible pour 2020 à : <https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/>. Pour 2021 à : <https://www.dlapiper.com/fr/france/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/>. Pour 2022 à : <https://www.dlapiper.com/en/us/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>. Pour 2023 : <https://www.dlapiper.com/en-au/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023>

⁴ Gartner Privacy report 2022

Ceci nous amène à interroger l'influence de possibles effets culturels dans les réponses des individus face à une violation de données personnelles. Nous questionnons, plus spécifiquement, l'importance de l'individualisme (e.g., la défense de ses propres buts et intérêts) comme valeur fondatrice du droit à la protection de la vie privée et des moyens de recours à ce droit.

Pour répondre à cette question, nous ancrons cette thèse dans le champ des recherches en vie privée (qui visent essentiellement à identifier les effets de la préoccupation pour le respect de la vie privée sur les intentions et comportements des individus en matière de divulgation de données personnelles), vues par le prisme des recherches en marketing (qui visent à analyser les relations avec les clients et usagers, à identifier des tendances managériales, à formuler des recommandations pour les entreprises et les politiques publiques). De cette manière, nous souhaitons mieux comprendre les réponses des individus face à une violation de leurs données personnelles, ainsi que les mécanismes psychologiques et sociologiques (intégrant notamment une préoccupation pour le respect de la vie privée) générant ces réponses. Cette recherche vise à renforcer la protection des usagers dans un contexte récent et anxiogène d'insécurité informatique accrue. Nous affirmons l'ambition d'ouvrir un champ entre vie privée et sécurité, et d'intégrer les questions de cybersécurité dans la recherche en marketing.

De plus, nous éclairons la compréhension de ces réponses à la lumière des effets culturels. Considérant alors la culture comme un ensemble de valeurs agissant à des niveaux macro (institutionnel), méso (sociologique) ou micro (psychologique), nous soutenons qu'une préférence culturelle pour des valeurs d'égalité sociale et de genre conduit les individus à adopter des réponses plus actives face à une violation de leurs données personnelles. Nous identifions alors des moyens d'action plus égalitaires et collectifs à proposer aux entreprises et collectivités, et notamment à travers le développement des pratiques sociales (Bourdieu, 1972; Giddens, 1984) de défense de la vie privée.

Notre introduction définit le cadre général dans lequel ces travaux sont conduits, concernant l'état des recherches actuelles (1), le périmètre défini des violations de données personnelles (2) et son positionnement dans le champ de la protection de la vie privée (3). Ceci nous amène à préciser la problématique et les objectifs de recherche (4), le plan de l'argumentation et la diversité méthodologique de la recherche (5), la thèse soutenue et les apports attendus (6), et enfin le plan général de la thèse (7).

1. Contextualisation de la recherche et état des recherches actuelles.

Notre travail interroge l'influence de possibles effets culturels dans les réponses face à une violation de données personnelles. La recherche montre clairement l'influence de la culture sur l'*information privacy concern* (Miltgen & Peyrat-Guillard, 2014; Smith et al., 2011), i.e., la possibilité pour un individu de contrôler l'utilisation potentielle par des tiers de ses données personnelles (Belanger et al., 2002; Westin, 1967). Mobilisant essentiellement la dimension de la culture nationale d'individualisme (i.e., une préférence pour la défense d'intérêts et d'objectifs personnels ; Hofstede, 1984), celle-ci étant considérée comme une dimension clé relative à la protection de la vie privée, les travaux attestent une plus grande préoccupation pour la protection de sa vie privée dans les pays plus individualistes. Or ceci conduit à déduire qu'une préférence pour collectivisme (dimension opposée à l'individualisme ; i.e., une priorité donnée à la cohésion du groupe social d'appartenance et à la loyauté envers celui-ci) implique un souci moindre de ses données personnelles (dont il serait alors possible d'abuser), ce qui soulève de nombreuses interrogations (Martin & Murphy, 2017). De plus, des résultats contradictoires apparaissent (e.g., un souci de protection de ses données plus important chez les étudiants chinois qu'américains, pourtant plus individualistes ; Lowry et al., 2011), appelant de nouvelles explorations susceptibles de varier les méthodologies et les référentiels culturels (e.g., Benamati et al., 2021; Martin & Murphy, 2017).

Par ailleurs, les réponses des individus à une violation de leurs données personnelles ont été très peu étudiées (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018). Premièrement, une typologie des réponses de protection de la vie privée est proposée (Son & Kim, 2008) mais n'a pas été actualisée depuis 2008. Deuxièmement, l'exploration du comportement du consommateur dans une situation de vulnérabilité informatique est nouvelle. En effet, la recherche en protection de la vie privée s'est surtout intéressée aux questions réglementaires (Westin, 1967; Solove, 2020) et de sécurité informatique (e.g., Bélanger & Crossler, 2011). Les comportements du consommateur sont explorés depuis une dizaine d'années, se focalisant sur l'influence d'une préoccupation pour la protection de la vie privée sur les comportements de divulgation ou non d'informations personnelles et leurs impacts sur les relations commerciales (Grosso et al., 2020; Martin & Murphy, 2017; Martin & Palmatier, 2020; Miltgen & Smith, 2019; Smith et al., 2011). Nous observons une émergence récente sur les questions de vulnérabilité du consommateur (i.e., une incapacité pour le consommateur d'atteindre ses objectifs, suite à une perte de contrôle et de liberté de choix ; Del Bucchia et al., 2021; Brough

& Martin, 2021; Cloarec, 2022). Troisièmement, les recherches portant sur les violations de données personnelles se sont intéressées aux causes et effets des violations pour les entreprises, en particulier sur leurs cours boursiers et risques réputationnels ou opérationnels (e.g., Confente et al., 2019; Khan et al., 2021; Malhotra & Kubowicz Malhotra, 2011; Rasoulilian et al., 2021; Romanosky et al., 2013). Des premiers travaux s'intéressent aux réactions des individus face à une violation de données personnelles, considérées comme des incidents de service (Rasoulilian et al., 2017). Par conséquent, de plus amples recherches sont attendues.

En synthèse (cf. Tableau 1), il existe une influence claire de la culture et notamment d'une préférence culturelle nationale pour l'individualisme (i.e., la défense de ses intérêts personnels) sur la préoccupation pour le respect de la vie privée. Cependant, les recherches n'expliquent ni certaines contradictions dans les résultats ni le souci de protection des données personnelles dans les pays valorisant davantage le collectivisme. En outre, concernant les réponses face à une violation de données personnelles, son impact sur le niveau de confiance des consommateurs est démontré et expliqué par certains phénomènes (e.g., sentiment de rupture de contrat) et une première typologie des réponses est proposée. Mais, les recherches n'explorent pas précisément les différentes réponses des individus spécifiquement dans le cas des violations de données et leurs mécanismes.

Tableau 1 : État des recherches

État des recherches	Aspects connus	Aspects inconnus
Culture et vie privée	- influence de la culture - influence d'une préférence culturelle nationale pour l'individualisme sur le souci de respect de la vie privée	- contradictions dans les résultats - souci de protection des données personnelles inexpliqué dans les pays valorisant le collectivisme
Réponses face à une violation de données personnelles	- première typologie des réponses - impact d'une violation de données personnelles sur le niveau de confiance des consommateurs (e.g., stress, sentiment de rupture de contrat)	- différentes réponses des individus dans le cas des violations de données inexplorées - mécanismes à enrichir

Avant de préciser notre problématique de recherche, il nous apparaît important de définir ce que sont les violations de données personnelles.

2. Périmètre des violations de données personnelles.

Le nombre de violations de données personnelles signalées a augmenté en France de 79% entre 2020 et 2021⁵ comme dans le reste du monde. En 2021, seuls 20% des entreprises ont déclaré ne pas avoir été attaquées informatiquement⁶ et 952,8 millions de personnes ont été victimes d'une violation de données personnelles dans le monde⁷. Toutes les entreprises et organisations sont touchées. Mais qu'est-ce qu'une violation de données personnelles ?

Le RGPD indique (Art. 4.12⁸) qu'« une violation de données est constituée par tout incident de sécurité, accidentel ou illicite, entraînant l'altération, la destruction, la perte ou la divulgation de données à caractère personnel ». De façon générale, une violation de données résulte d'un accident technique ou d'un vol. Celui-ci peut être compris selon :

- Le support accidenté ou volé,
- L'intention, i.e., qui est à l'origine de l'incident technique ou du vol ?
- La cible,
- Le préjudice de la violation, i.e. « à qui profite le crime ? »

Premièrement, l'incident ou le vol peut être physique (e.g., vol de matériel informatique permettant l'accès à des données comme un disque dur ou une carte bancaire) ou logique (e.g., logiciel malveillant ouvrant des portes informatiques permettant l'accès à des données) (Khan et al., 2021). Nous considérons dans cette thèse ces deux cas, car ce ne sont que des moyens à déployer pour répondre aux mêmes intentions.

Deuxièmement, la violation de données personnelles peut être intentionnelle (e.g., pirates informatiques, collecte et traçage de données personnelles sans le consentement des personnes) ou non intentionnelle comme des accidents d'utilisation (e.g., logiciels défectueux endommageant le système, activation d'un logiciel envoyé par un mail « fishing ») (Khan et al., 2021). Or dans cette seconde option, la personne cliquant malencontreusement sur un lien dans un e-mail reçu est-elle responsable de la violation de données ? Ou bien encore donne-t-elle clairement son consentement éclairé à l'utilisation des données personnelles transmises par erreur en cliquant sur ce lien de « fishing » ? Nous pensons que non et nous intégrons ces deux

⁵ Rapport d'activités CNIL 2021 (disponible à : <https://www.cnil.fr/fr/la-cnil-public-son-rapport-dactivite-2021>)

⁶ Acronis Cyberthreats Report 2022 (disponible à : <https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/>)

⁷ <https://www.lebigdata.fr/violation-de-donnees-2021>

⁸ <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4>

possibilités dans notre définition des violations de données personnelles. Ceci aura un impact sur le positionnement général de la thèse que nous précisons ensuite.

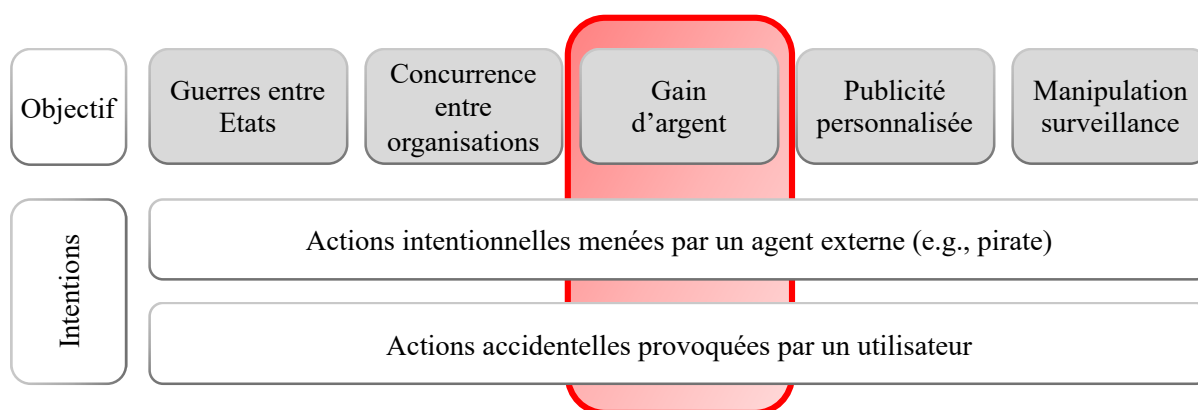
Troisièmement, une violation de données personnelles peut cibler des États, des organisations ou entreprises (Confente et al., 2019; Rasoulilian et al., 2021) ou des individus (Solove & Hartzog, 2022). Notre thèse s'intéresse exclusivement aux individus.

Par conséquent, et quatrièmement, notre recherche exclut les violations de données visant des actions de renseignement dans le cas d'une guerre entre États, ou de concurrence entre organisations étatiques ou économiques. Hormis cela, les violations de données personnelles peuvent avoir pour objectifs (i) un gain d'argent (e.g., revente directe des données personnelles ou demande de rançon, notamment en faisant jouer les risques de préjudices réputationnels ou psychologiques ; Citron & Solove, 2021), (ii) faire de la publicité personnalisée, (iii) manipuler ou surveiller les populations. Nous excluons de cette définition l'utilisation non autorisée des données personnelles à des fins de ciblage publicitaire (comme l'utilisation des cookies tiers), de manipulation comportementale ou de surveillance des populations (Zuboff, 2019), reposant en particulier sur les modèles économiques des géants du numérique (e.g., Alphabet, Meta) fondés sur la collecte et l'usage de données personnelles (Véliz, 2020). Notre recherche considère uniquement les gains d'argent.

Ainsi dans notre thèse, une violation de données personnelles est un vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif.

La Figure 1 ci-dessous illustre ce que cette définition intègre ou non :

Figure 1 : Définition des violations de données personnelles



Ceci étant défini, l'éventail des incidents pouvant être considérés comme des violations de données personnelles est très large, tant par les caractéristiques des données personnelles volées que par les acteurs et les actions provoquant ces violations. Notre recherche vise à représenter cette diversité à travers les situations mobilisées dans les essais : vol de données de santé dans le deuxième essai (chapitre 5), vol de données d'un site marchand et vol de données bancaires dans le troisième essai (chapitre 6).

Nous souhaitons attirer l'attention du lecteur sur trois points :

- (i) dans le premier essai (chapitre 4), nous ne connaissons pas les motifs de plainte pour violations de données personnelles déposées auprès du régulateur (CNIL), même si de grandes tendances sont communiquées par la CNIL (i.e., prioritairement plaintes pour publicités intrusives et surveillance au travail ; cf. Annexe 10),
- (ii) le sujet des violations de données personnelles a beaucoup évolué au cours de la période de rédaction de cette thèse, rendant la consistance de l'analyse complexe,
- (iii) notre thèse n'approfondit pas la compréhension par les usagers des différentes formes de violations de données personnelles, ce qui permettrait d'en compléter sa définition.

Tant la contextualisation de notre recherche que le périmètre défini des violations de données personnelles influencent le positionnement souhaité de notre recherche, que nous précisons dans la partie suivante.

3. Positionnement de la recherche : en protection de la vie privée.

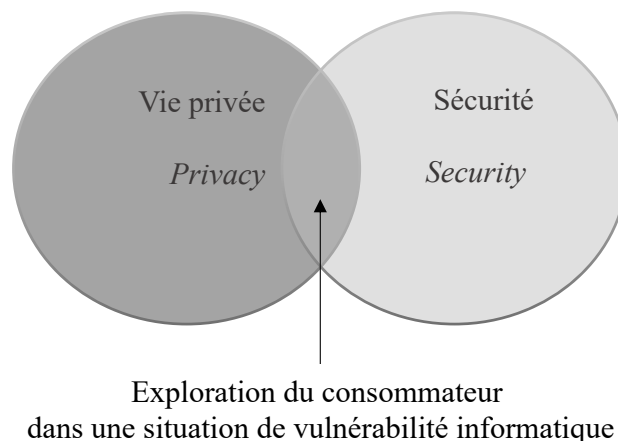
Notre sujet, portant sur l'influence de la culture sur les réponses des individus face à une violation de leurs données personnelles, est un sujet de vie privée à explorer en marketing.

En effet, le champ de la vie privée (*privacy*) vise à comprendre le lien entre préoccupation pour le respect de la vie privée et comportement individuel. La *privacy*, (ou vie privée informationnelle) est définie comme le droit de contrôler les informations sur soi-même (Westin, 1967). Cette notion de contrôle de données personnelles est étudiée en droit (aboutissant aux obligations réglementaires d'obtenir le consentement des usagers pour collecter et utiliser leurs données), en systèmes d'information, et en marketing depuis environ vingt ans (Martin et al., 2021). L'échange d'informations personnelles entre entreprises et consommateurs est alors compris comme un contrat social implicite (e.g., Milne, 2000) dans le cadre duquel l'individu est plus ou moins conscient de la valeur de l'échange. C'est pourquoi les travaux en *privacy* s'intéressent aux effets de la préoccupation pour le respect de la vie privée (*privacy concern*) sur les comportements des individus (e.g., Dinev et al., 2006; Milberg et al., 1995). Enfin, les recherches en *privacy* insistent récemment sur les questions de perte de contrôle et donc de vulnérabilité des individus (Del Bucchia et al., 2021) dans un contexte de digitalisation accrue de nos économies, de risques croissants de sécurité informatique et de violations de données personnelles (Rasoulilian et al., 2021). Notre recherche fait écho à ces récents travaux.

Nous ancrons cette recherche sur la protection de la vie privée dans le champ du marketing. Ceci nous permet, d'une part, d'éclairer nos questionnements à la lumière des connaissances sur les relations clientèle et en particulier sur les réactions d'insatisfaction des consommateurs-usagers (Grégoire et al., 2009; Grégoire & Fisher, 2008) et, d'autre part d'inscrire notre recherche dans un champ visant à adresser les enjeux économiques et sociétaux de certaines pratiques (Martin et al., 2021) ainsi qu'à identifier des actions possibles pour les entreprises et les politiques publiques afin de mieux protéger l'utilisateur-consommateur (e.g., Parguel et al., 2017, 2018). Cette approche enrichit plusieurs questionnements visant à « diffuser une culture de la cybersécurité auprès de l'opinion publique non pas pour transformer chaque citoyen en informaticien, mais bien pour en faire un consommateur de technologies responsable, conscient de l'ampleur de la menace potentielle et de la valeur de l'information. » (Arpagian, 2022, p.123)

En effet, si notre recherche ne se positionne pas en sécurité informatique (i.e., un champ étudiant tous les éléments informatiques permettant de stocker et de transférer des informations numériques tout en protégeant leur intégrité et en protégeant les données, réseaux et infrastructures de toute menace venue du cyberspace), la frontière entre protection de la vie privée et sécurité est de plus en plus ténue au regard des risques informatiques actuels. Ainsi à ce jour, Dinev (2014) préconise d'accentuer les recherches portant sur un juste équilibre entre vie privée (i.e., le juste niveau de protection de vie privée acceptable et nécessaire), commodité (des biens et des services, notamment la personnalisation des services) et sécurité (protection de différents dangers, comme par exemple la surveillance des populations ; Zuboff, 2019). C'est pourquoi nous pensons que notre recherche pourrait adopter un positionnement en sociologie de la cybersécurité, similaire à ce que la sociologie de la santé est à la médecine, et visant donc à mieux comprendre les interactions entre la société (et les individus qui la composent) et les risques liés à la sécurité informatique (portant notamment sur la perte de vie privée), afin de proposer des pratiques et actions pour soutenir le développement d'une cybersécurité efficace.

Au-delà des contributions théoriques de cette recherche, nous affirmons le souhait de contribuer fortement à développer les questions de sécurité dans le champ de la vie privée, à travers l'exploration du consommateur (usager) dans une situation de vulnérabilité informatique.



Pour finir, notre recherche vise à éclairer ces comportements à la lumière des effets culturels. Nous nous appuyons alors sur les connaissances portant sur la culture issues du management interculturel et international, sans chercher à y contribuer particulièrement. Grâce à cela, nous adoptons une analyse multi-niveaux et une diversité méthodologique précisée par la suite.

4. Problématique et objectifs de la recherche.

L'état de la littérature met en exergue, d'une part, la nécessité d'interroger plus précisément l'influence indéniable de la culture sur la préoccupation pour le respect de la vie privée, en particulier le rôle d'une préférence culturelle pour l'individualisme (i.e., une préférence pour la défense d'intérêts et d'objectifs personnels). D'autre part, les réactions des individus à une violation de leurs données personnelles (définies comme un vol illégal d'informations confidentielles) ont très peu été explorées en marketing, dans un contexte croissant d'insécurité informatique.

Notre recherche adresse donc la question suivante :

Quelle est l'influence de la culture sur le comportement de réponse face à une violation de ses données personnelles ?

Plus précisément, notre thèse pose trois questions, auxquelles la recherche ne répond à ce jour pas encore suffisamment :

- (i) Quelles sont les réponses face à une violation de données personnelles ?
- (ii) Quelle est l'influence de la culture sur ces réponses ?
- (iii) Quels mécanismes psychologiques et sociologiques relient la culture aux réponses ?

Notre recherche vise à observer les effets culturels afin de mieux éclairer les réponses et les mécanismes psychologiques et sociologiques. Ainsi, les effets culturels structurent notre thèse. Plus précisément, nous faisons le choix de considérer la culture comme un ensemble de valeurs universelles, implicites, des symboles qui donnent du sens à l'action et à la décision (Rokeach, 1973; Schwartz, 2006). Nous considérons que les valeurs culturelles opèrent à trois niveaux : macro (institutionnel), méso (social) et micro (psychologique) (Livian, 2011; Martin & Palmatier, 2020; Matsumoto, 2007). Nous optons pour une approche multi-niveaux (macro, méso et micro) avec une diversité méthodologique pour chaque niveau. Nous précisons cela dans la partie suivante.

5. Plan de l'argumentation et cadre méthodologique de la recherche.

Notre thèse est composée essentiellement de trois essais, chacun correspondant à un niveau d'observation : macro (institutionnel), méso (social) et micro (psychologique). Pour chacun de ces essais, notre objectif est de proposer une diversité théorique et méthodologique.

En effet, notre recherche présente un double enjeu : aller dans la continuité d'un champ encore peu exploré pour compléter les recherches actuelles, mais également faire preuve d'originalité et savoir « faire un pas de côté », pour apporter un éclairage nouveau aux connaissances actuelles. De plus, une approche qualitative et exploratoire est nécessaire pour éclairer un champ relativement nouveau et appréhender avec un regard généralement positiviste. Il en découle un positionnement post-positiviste (juste équilibre entre des approches positivistes et interprétativistes ; Cooper, 1997) qui permet au chercheur d'interroger son propre système de valeurs.

Par conséquent, nous mobilisons un cadre théorique déjà connu : théorie de la distance psychologique (Trope & Liberman, 2010) (essai micro), mais peu interrogé dans le cadre des influences culturelles. L'essai méso repose, quant à lui, de façon totalement novatrice sur le cadre théorique de la pratique (Bourdieu, 1972; Giddens, 1984).

De plus, notre thèse de doctorat, s'appuyant sur des données tant quantitatives que qualitatives, s'articule autour de trois approches empiriques :

- Une première approche quantitative, à l'aide d'une base de données open-source ;
- Une deuxième approche qualitative, basée sur une série d'entretiens (N=15), nous permettant d'approfondir la compréhension de certains phénomènes de réponses pour la protection de données personnelles face à une violation de données ;
- Une troisième approche quantitative (N=452), hypothético-déductive.

6. Thèse soutenue et apports attendus de la recherche.

Dans cette thèse, nous soutenons qu'**une préférence culturelle pour des valeurs d'égalité sociale et de genre amène les individus à adopter des réponses plus actives face à une violation de leurs données personnelles**. Deux autres motivations culturelles sont identifiées : la liberté et la sécurité. Nous montrons que cette préférence opère à trois niveaux d'observation : (1) macro, le cadre institutionnel amenant les individus résidant dans des pays valorisant l'égalité des genres à davantage porter plainte, (2) méso, la protection de la vie privée étant envisagée comme une pratique sociale mobilisant des techniques, des compétences et des idéaux comme la défense de l'égalité sociale, (3) micro, l'égalité sociale et de genre étant des valeurs culturelles impliquant moins de distance psychologique avec la violation de données. Ces résultats permettent d'apporter des contributions théoriques et pratiques fortes.

Contributions théoriques :

Notre recherche porte des contributions théoriques novatrices aux recherches en vie privée :

- (i) une compréhension différente des phénomènes et effets reliant culture et protection de la vie privée informationnelle, avec la prépondérance d'un souci d'équité sociale ;
- (ii) un éclairage des réponses du consommateur dans une situation de vulnérabilité informatique et du lien entre vie privée et sécurité, avec la proposition d'une typologie de réponses aux violations de données personnelles ;
- (iii) un enrichissement des recherches sur la distance psychologique avec la vie privée, montrant son importance dans les réponses face à une violation ;
- (iv) l'identification de la théorie de la pratique, qui apporte un cadre éclairant pour le développement de pratiques sociales de protection de la vie privée, mobilisant des techniques, des compétences et des idéaux.

Ces différents éclairages théoriques (équité sociale, lien entre vie privée et sécurité, importance de la distance psychologique, et pratique d'une protection de la vie privée) nous permettent d'enrichir notre compréhension de la préoccupation pour la protection de la vie privée, envisagée comme un « mieux vivre ensemble » et non un « mieux vivre tout seul ». Ainsi, **être soucieux de la protection de sa vie privée, ce n'est pas vouloir contrôler ses propres données personnelles, c'est vouloir sécuriser les données personnelles de tous**. Ceci permet d'alimenter les réflexions en cours sur une reconceptualisation de *l'information privacy concern* (e.g., Bansal & Nah, 2022 ; Martin et al., 2017).

Implications pratiques :

Ces contributions théoriques permettent d'imaginer des implications pratiques fortes. Les résultats de notre recherche identifient des possibilités d'actions à destination des décideurs politiques (e.g., Commission européenne, CNIL), des différents acteurs du numérique (e.g., entreprises, structures éducatives, collectivités, médiateurs numériques), et des acteurs de la cybersécurité dans leur souhait de prévenir les comportements humains pour renforcer la sécurité informatique. Les implications pratiques que nous proposons s'inscrivent dans un cadre général de développement de pratiques de protection de la vie privée à un niveau méso, autour des notions de **responsabilité et sécurité**.

Nous abordons plusieurs propositions d'actions, suggérons des initiatives en termes de communications publicitaires et médiatiques, et discutons des modifications à apporter aux réglementations, selon les trois axes de résultats :

- Sur la base de nos résultats portant sur les réponses aux violations, favoriser (i) les possibilités de plaintes aux régulateurs, (ii) la responsabilité des entreprises dans l'identification des violations, (iii) identifier les améliorations possibles pour chaque réponse ;
- Pour prendre en compte les effets culturels identifiés (équité, liberté, sécurité), (i) développer des actions de communication, (ii) développer des moyens d'action autour du « mieux vivre ensemble », (iii) adapter les moyens d'action selon les groupes sociaux, (iv) adapter localement les réglementations globales et développer des moyens de recours au droit plus collectifs ;
- Pour prendre en compte les mécanismes sociologiques et psychologiques, (i) développer une feuille de route basée sur la théorie de la pratique, (ii) développer des actions incluant la réduction de la distance psychologique.

Limites de la recherche :

Notre recherche a plusieurs limites, qui sont autant de voies de recherches futures. Par exemple, elle n'apporte pas une réponse à la compréhension des différences culturelles entre des pays, notamment dans les pays émergents comme l'Inde ou l'Afrique, en réponse à l'appel de Martin & Murphy (2017). Elle n'identifie pas non plus les critères permettant à un utilisateur de définir une violation de données personnelles. Enfin, certains points méthodologiques concernant les théories de la pratique ou de la distance psychologique peuvent être améliorés.

7. Plan de la thèse

Notre thèse est composée de 7 chapitres que nous décrivons dans ce dernier paragraphe.

Le **premier chapitre (1)** est une introduction générale au cours de laquelle nous précisons le contexte managérial (violations de données personnelles et réglementations pour la protection de données personnelles) et le contexte académique de la thèse (causes et effets des violations de données puis culture et souci de protection de données personnelles).

Dans un **deuxième chapitre (2)**, nous précisons les fondements théoriques de notre recherche autour de trois axes :

- la protection des données personnelles, montrant que le souci de protection de ses informations personnelles est un concept abstrait,
- les réponses des consommateurs insatisfaits, montrant que les réponses face à une violation de données personnelles peuvent faire appel à d'autres antécédents tels que le sentiment de capacité individuelle ou la pression sociale à agir ;
- la culture et les valeurs culturelles, montrant que la culture est une conscience collective composée de valeurs, socle de nos décisions, actions et institutions, au-delà de toutes frontières nationales.

Fort de ces fondements, nous fixons dans le **troisième chapitre (3)** le cadre général de la thèse, les questions de recherche, le cadre théorique, le positionnement épistémologique et les méthodologies de recherche.

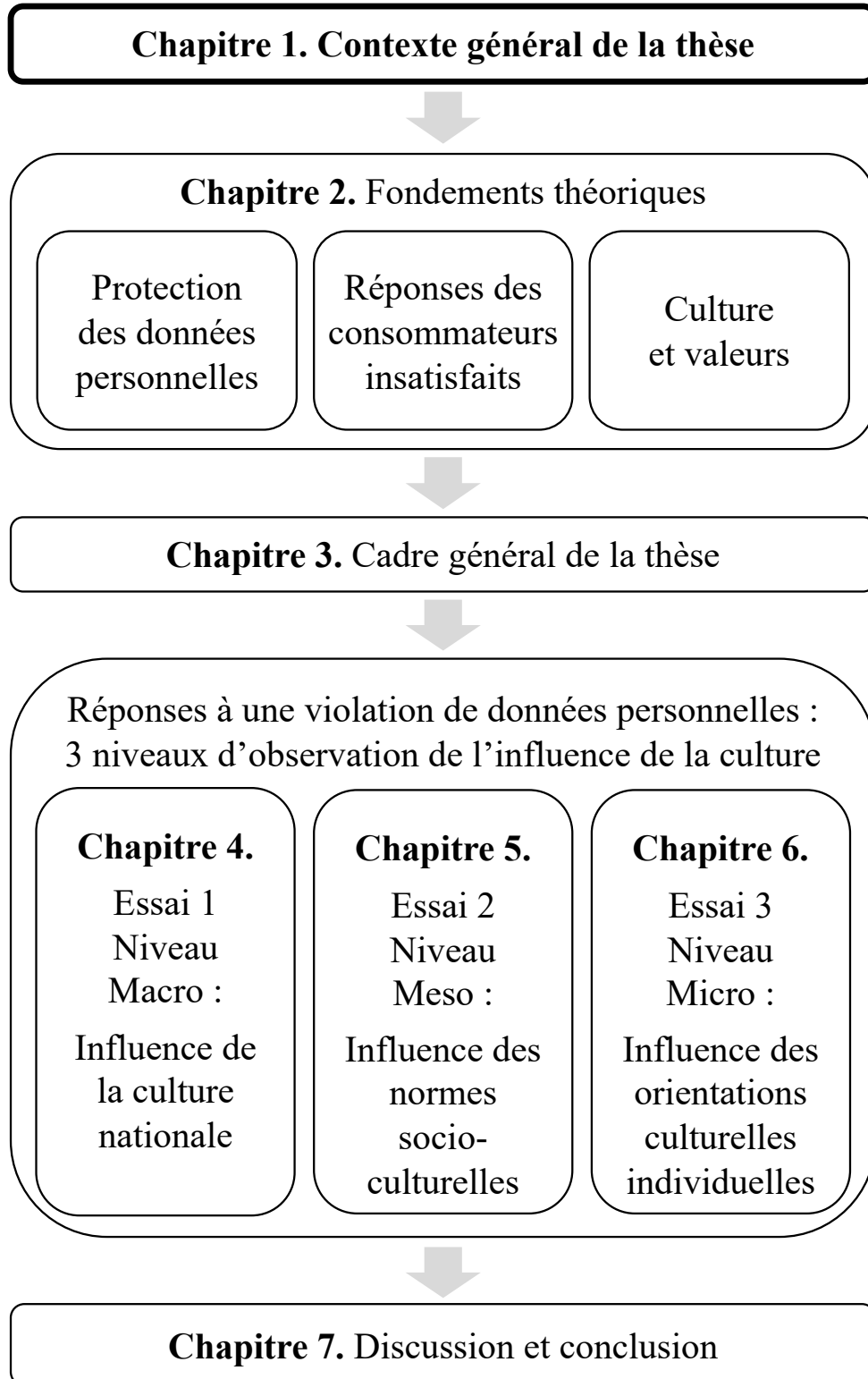
Les trois chapitres suivants (chapitres 4 à 6) correspondent chacun à un essai qui compose cette thèse de doctorat. Dans un **premier essai (niveau macro – chapitre 4)**, nous interrogeons le rôle des macro-normes institutionnelles et l'influence de la culture nationale. Nous mobilisons une base de données recensant des plaintes déposées pour violation de données personnelles auprès des autorités européennes de protection des données personnelles (e.g., CNIL en France), base de données enrichie des dimensions culturelles d'Hofstede (Hofstede, 1984, 2001; Hofstede et al., 2010). Nous observons que les individus vivant dans des pays européens valorisant davantage la féminité (i.e., l'égalité des sexes et les soins communautaires) ont tendance à porter plainte davantage, de même – mais dans une moindre mesure – que ceux vivant dans des pays européens valorisant davantage l'individualisme ou la tradition.

Dans un **deuxième essai (niveau méso – chapitre 5)**, nous mobilisons des entretiens approfondis (N=15) et montrons, à la lumière de la théorie de la pratique (Bourdieu, 1972; Giddens, 1984), que la défense d'une équité sociale est une motivation essentielle à l'adoption d'une réponse active. Deux autres modèles de motivation sont identifiés (reposant sur la défense de liberté ou de sécurité). La protection de la vie privée est alors envisagée comme une pratique sociale et collective, mobilisant des moyens techniques, des compétences (e.g., sentiment d'efficacité) et des valeurs. Cette recherche apporte alors un éclairage théorique totalement novateur, car elle envisage la protection de la vie privée comme une pratique sociale, et non comme une pratique individuelle, éliminant l'idée que les individus sont les seuls responsables. D'autre part, elle remet en question l'importance d'une préférence pour l'individualisme comme valeur fondatrice de la protection des données personnelles.

Dans un **troisième essai (niveau micro – chapitre 6)**, nous appliquons la théorie de la distance psychologique (Trope & Liberman, 2010) pour explorer les mécanismes psychologiques reliant orientations culturelles individuelles et réponses du consommateur face à la violation de ses données personnelles. À l'aide d'une enquête en ligne adressée à un large échantillon de Français (N=452), nous confirmons nos premiers résultats et montrons que l'égalité sociale et l'égalité de genre sont les valeurs culturelles qui influencent le plus les réponses, impliquant moins de distance psychologique avec la violation de données personnelles et favorisant des réponses techniques concrètes ; tandis que d'autres orientations, comme l'indépendance, n'encouragent que la préoccupation pour la protection de ses données personnelles tout en favorisant des réponses sociales ou institutionnelles.

Pour finir, une **conclusion générale (chapitre 7)** inclut une discussion sur nos résultats, les contributions, les limites et les voies de recherche possibles de notre travail.

Structure générale de la thèse



Chapitre 1. Contexte général de la recherche



Ce premier chapitre introductif a pour objectif de présenter le contexte tant managérial qu'académique de notre recherche portant sur l'influence de la culture sur les réponses face à une violation de données personnelles.

Dans une première section, nous dresserons un tableau des violations de données personnelles : combien de personnes touchent-elles ? Comment se produisent-elles ? comment peuvent-elles être réglées ? Ceci nous permet de réaffirmer les définitions données en introduction, mais également de les illustrer. Face à ces violations, des réglementations internationales pour la protection des données personnelles sont établies (e.g., RGPD). Nous les détaillerons, en mentionnant notamment la grande variabilité dans le nombre de plaintes entre pays européens, laquelle conduit à nous interroger sur l'influence de possibles variables culturelles dans le comportement de réponse face à une violation de données personnelles.

Dans cette perspective, des recherches se sont intéressées aux causes et aux effets des violations de données personnelles pour les entreprises, étudiant peu les réponses des individus à une violation de leurs données personnelles (Mamonov & Benbunan-Fich, 2018). D'autres recherches ont également étudié l'influence de la culture sur la préoccupation pour la protection de la vie privée. Nous exposerons dans une deuxième section l'état des recherches sur ces deux aspects.

La troisième section formule les axes de recherche poursuivis dans cette thèse, ainsi que nos trois principales questions de recherche qui sont : (i) Quelles sont les réponses face à une violation de données personnelles ? ; (ii) Quelle est l'influence de la culture sur ce comportement de réponse ? ; (iii) Quels sont les mécanismes psychologiques et sociologiques reliant la culture aux réponses adoptées face à une violation de données personnelles ?

Section 1. Contexte managérial de la recherche

Cette section portant sur le contexte managérial de notre thèse comporte deux parties : la première partie expose le cadre général des violations de données personnelles, la seconde présente les réglementations internationales pour la protection des données personnelles⁹.

1. Violations de données personnelles : le « far-west »

Dans cette partie sur les violations de données personnelles, nous avons 4 objectifs : définir ce que sont les données personnelles (1.1.) et les violations de données personnelles (1.2.), en complément de définitions apportées en introduction, souligner leur diversité (1.3) et les volumes importants et à la hausse de données violées (1.4), exposer le contexte de criminalité dans lequel ces violations s'inscrivent et les moyens mis en œuvre pour les résoudre (1.5) et comprendre le lien entre cybercriminalité et protection des données personnelles (1.6.)

1.1. Définition et classification des données personnelles

1.1.1. Définition des données personnelles

La Commission Nationale Informatique et Libertés (CNIL) en France définit une donnée personnelle comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique peut être identifiée : (i) directement (e.g., nom et prénom), (ii) indirectement (e.g., par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image). L'identification d'une personne physique peut être réalisée : (i) à partir d'une seule donnée (exemple : nom), (ii) à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association). Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son*

⁹ Les chapitres 1 et 2 de notre thèse reprennent certains points et idées extraites du chapitre « Privacy Regulation in the Age of Artificial Intelligence » (Aubert-Hassouni & Cloarec, 2022). Ces idées ont été réarticulées et reformulées pour permettre une bonne intégration dans le manuscrit de thèse.

adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie@email.fr ») ne sont pas, en principe, des données personnelles »¹⁰.

Cette définition proposée par la CNIL implique que les informations peuvent être de toute nature : papier, manuscrite ou électronique, par exemple. Cependant, la digitalisation des vies personnelles et économiques, représentée par le volume croissant de données stockées, créées et répliquées dans le monde, passant de 2 à 64 zettaoctets entre 2010 et 2020¹¹, montre que ces données sont dorénavant essentiellement numériques et digitales.

D'autre part, une donnée est personnelle car elle permet d'identifier une personne. Une donnée personnelle se distingue des données professionnelles, telles que les brevets ou les secrets professionnels. En revanche, toutes les informations portant sur des clients, salariés et collaborateurs, voire patients, sont bien des données personnelles.

1.1.2. Classification des données personnelles

Comme présenté dans le Tableau 2 ci-après, certaines données permettent l'identification directe de la personne (« données objectives ») alors que d'autres identifient, en premier lieu, des attitudes et des comportements (« données subjectives ») (Rochelandet, 2010). Cependant, des recherches déjà anciennes (2009) indiquent que des informations sensibles comme un numéro de sécurité sociale (SSN) peuvent être retrouvées en quelques secondes à partir d'une photo prise d'une personne inconnue, d'un profil Facebook et d'une base de données de numéros SSN (Acquisti & Gross, 2009). De ce fait, *« toute information personnelle peut être une information sensible »¹².*

¹⁰ <https://www.cnil.fr/fr/definition/donnee-personnelle>

¹¹ <https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde>

¹² TED Talk d'Alessandro Acquisti, 18.10.2013, What will a future without secrets look like? (accessible à : https://www.youtube.com/watch?v=H_pqhMO3ZSY&t=753s)

Tableau 2 : Données personnelles objectives et subjectives (Rochelandet, 2010)

Type de données		Exemples
Données objectives	Données d'identification et de contact	Adresse postale Permis de conduire Numéro de carte d'identité ou carte vitale
	Données physiques et de signalement	Situation médicale Photographie, voix
	Données sociodémographiques	Date de naissance
	Données juridiques	Casier juridique
	Données financières et foncières	Solde de compte bancaire
Données subjectives	Préférences et centres d'intérêt	Orientation sexuelle
	Opinions et activités politiques, religieuses et syndicales	Opinions politiques
	Données comportementales	Achats Consommation d'électricité
	Données géographiques	Enregistrement par bornes de contact dans malls Données de localisation
	Données relationnelles	Réseaux sociaux

Par ailleurs, les données peuvent être collectées de différentes manières : formulaires en ligne (e.g., formulaire d'abonnement à un service, à un programme de fidélité), informations divulguées publiquement (e.g., blogs et réseaux sociaux), traces collectées à l'insu de la personne et tromperie (e.g., *cookies*, géolocalisation, piratage de base de données, phishing), informations divulguées à des tiers (e.g., achat de base de données), données obtenues par recoupement, etc. (Rochelandet, 2010).

Nous identifions 3 types de données :

- *Données obligatoires*, car leur communication est imposée de façon obligatoire à l'individu (e.g., données de santé, données administratives, données fournies à l'employeur),
- *Données intentionnelles*, car communiquées intentionnellement par l'individu sans être forcément obligatoires (e.g., sur des applications ou dans le cadre de programmes de fidélité, sur les réseaux sociaux),
- *Données cachées*, car collectées en mode 'black box' (e.g., cookies tiers). En effet, une part importante des données personnelles sont collectées à l'aide de cookies tiers au

point que le marché publicitaire Internet mondial (468.05 milliards d'euros en 2022¹³), se retrouve très perturbé en Europe par l'interdiction des cookies tiers imposée par le RGPD¹⁴.

De cette typologie de données personnelles, nous distinguons 3 types d'accès aux données personnelles (cf. Figure 2) :

- Les accès autorisés (pour les données obligatoires et les données intentionnelles),
- Les accès non autorisés (pour les données cachées),
- Les accès violés (suite à un accident technique ou à un vol, dans le cas d'une violation de données personnelles, que nous précisons dans le paragraphe 1.2 ci-après).

Enfin, les données personnelles peuvent être utilisées pour différents usages.

Dans notre thèse, notre définition des données personnelles est la suivante :

Une donnée personnelle est une information confidentielle sur une personne physique, quel que soit le support sur lequel elle est disponible (e.g., digital, papier), le degré de précision permettant l'identification de la personne physique (e.g., objectif, subjective) et son degré de sensibilité (e.g., photo, donnée de santé).

¹³ <https://fr.statista.com/outlook/dmo/digital-advertising/worldwide>

¹⁴ Les cookies sont des fichiers déposés et stockés sur le navigateur web d'un internaute lors d'une première visite, permettant ensuite de le reconnaître. Ils peuvent être de *first party*, i.e., « natifs », et servent à optimiser la navigation de l'Internaute, ou *second* ou *third party*, collectés pour revente à des partenaires, servant alors à optimiser le ciblage et la personnalisation d'offres commerciales. Les cookies tiers collectent donc des informations sans le consentement clair et éclairé des utilisateurs : le RGPD impose donc de les supprimer. Or tout le modèle économique et le fonctionnement des acteurs de la publicité en ligne repose sur les cookies tiers. Par ailleurs, les cookies tiers sont principalement collectés par les moteurs de recherche : compte tenu de sa position dominante sur le marché du *search*, Google est le premier impacté par une baisse très importante de futurs revenus publicitaires liés à la suppression des cookies tiers. Par conséquent, Google cherche une solution de contournement, en a proposé certaines (e.g., Privacy Sandbox, FLoC) mais sans succès et vient d'annoncer en juillet 2022 un second report de la date de suppression des cookies tiers ... à 2024. De plus, cette interdiction fait l'objet de débats sur son efficacité : ainsi le RGPD a permis une réduction du volume de données partagées en ligne, mais a eu pour conséquence de favoriser la concentration de fournisseurs offrant des services d'assistance aux sites web, enregistrant une baisse du nombre de sociétés de 15% (Johnson et al., 2022).

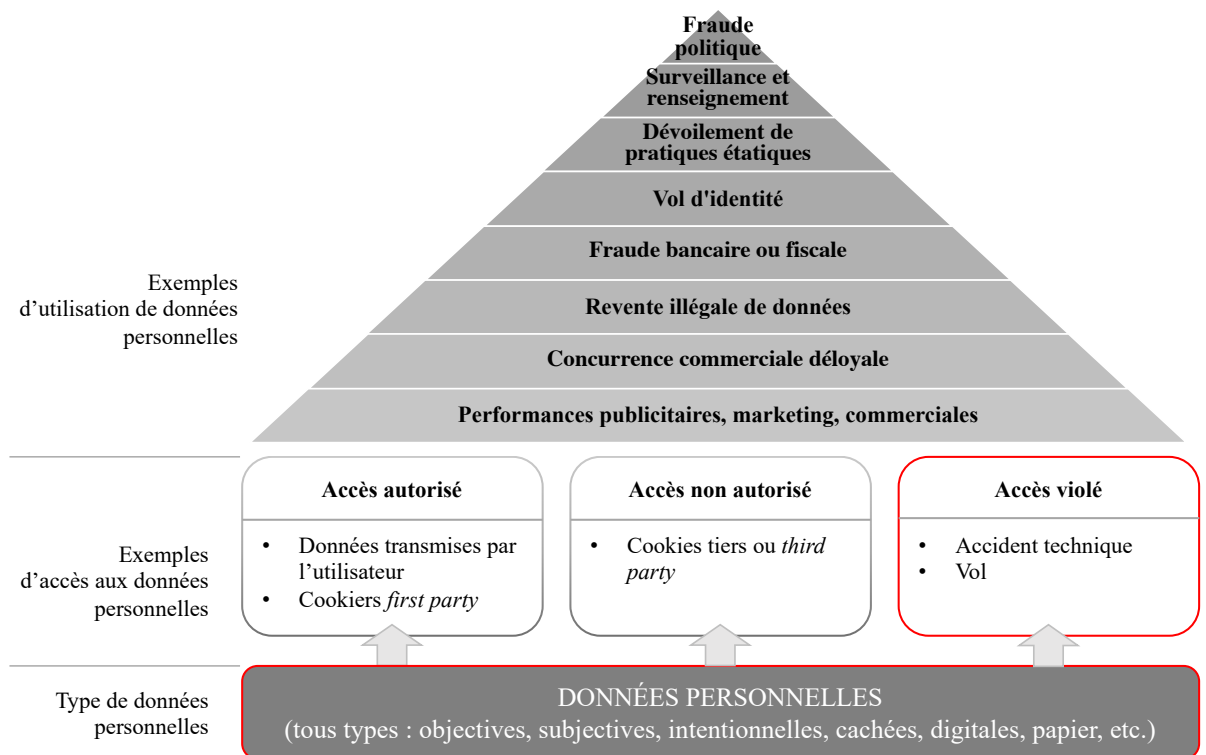
1.1.3. Utilisation des données personnelles

Les données personnelles sont des informations précieuses pour les marketeurs leur permettant de connaître le profil et les habitudes de chaque individu, d'adresser le bon message au bon moment et à la bonne personne, et donc d'optimiser les performances publicitaires et commerciales. Les données personnelles peuvent être utilisées, par exemple, pour des offres contextualisées (e.g., mise en relation de personnes en mobilité, promotion de services à proximité) ou des offres personnalisées. Ces possibilités de personnalisation peuvent être utiles pour les utilisateurs (e.g., gestion de la relation client) mais également aller à l'encontre de leurs intérêts : e.g., discrimination par les prix, polices d'assurance, prêts bancaires.

Si les marketeurs ont rapidement identifié l'utilisation qu'ils pouvaient faire des données personnelles (surtout avec l'apparition des cookies Internet, et à la même période des cartes de fidélité des enseignes), leurs techniques ont aussi été utilisées à des fins de fraude politique (ciblage d'électeurs potentiels et détournement d'opinions politiques). Ces pratiques ont généré un véritable marché de la donnée (e.g., data brokers, ChoicePoint).

Par ailleurs, le vol ou la falsification de données peut être pratiqué dans un objectif de concurrence commerciale déloyale, d'utilisation illégale ciblée (e.g., usurpation d'identité, fraude bancaire), de surveillance et renseignements (e.g., fichage par les administrations). Nous indiquons ces différents usages possibles sur la figure ci-dessous.

Figure 2 : Classification des types, accès et utilisations de données personnelles



Notre recherche porte sur : (i) tous les types de données personnelles, (ii) uniquement les accès aux données violés (violations de données) (entouré en rouge dans la Figure 2 ci-dessus), (iii) tous les modes d'utilisation de données.

1.2. Définition des violations de données personnelles

Une violation de données personnelles est une infraction qui va avoir pour conséquence de porter atteinte à la vie privée :

- Une atteinte est un dommage matériel ou moral¹⁵. L'atteinte à la vie privée est une expression juridique désignant le fait pour une personne d'être victime d'une violation de son droit au respect de la vie privée. La notion de vie privée est abordée dans l'article 9 du Code civil français : « Chacun a droit au respect de sa vie privée. Les juges peuvent sans préjudice de la réparation du dommage subi prescrire toutes mesures telles que séquestres, saisies et autres, propres à empêcher ou à faire cesser une atteinte à la vie privée ; ces mesures peuvent, s'il y a urgence, être ordonnées en référé. ». Aucune définition de la vie privée n'a été statuée par le législateur, laissant la possibilité aux juges de régler les contentieux par voie de jurisprudence ;
- « Une violation de données personnelles est constituée par tout incident de sécurité, accidentel ou illicite, entraînant l'altération, la destruction, la perte ou la divulgation de données à caractère personnel. » (Art. 4.12 du RGPD¹⁶)

Une violation de données personnelles résulte donc d'un accident technique ou d'un vol. Pour cette raison, nous distinguons accès non autorisé (e.g., collecte d'informations de profilage avec des cookies tiers) et accès violé aux données personnelles (e.g., vol d'informations par action de phishing) (cf. Figure 1) : notre recherche porte uniquement sur les données personnelles violées.

Nous avons, en introduction, apporté une définition des violations de données personnelles, que nous n'expliquerons pas de nouveau ici, mais que nous citons à nouveau :

Dans notre thèse, une violation de données personnelles est un vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif.

¹⁵ <https://dictionnaire.lerobert.com/definition/atteinte>

¹⁶ <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4>

Nous ajoutons cependant quelques informations concernant le lien entre les violations de données personnelles et pratiques de la publicité digitale. Il existe, en effet, actuellement un débat ardent sur la légalité des pratiques de la publicité digitale (e.g., publicité programmatique, système d'enchères, analyse de trafic web), qui repose principalement sur l'exploitation de données personnelles fournies par les cookies tiers. Le RGPD a imposé certaines règles (e.g., consentement obligatoire) et interdit les cookies tiers. Cette interdiction des cookies tiers a souvent été reportée pour éviter de déstabiliser le marché publicitaire mondial. Également, en janvier 2022, l'autorité autrichienne de protection des données personnelles a jugé l'utilisation de Google Analytics contraire au RGPD¹⁷ et a été suivie par ses homologues européens. De plus, l'Irish Council for Civil Liberties a dévoilé en mai 2022 que des informations de géolocalisation ou d'historique de navigation sont collectées et revendues à des data brokers, assimilant ainsi certaines pratiques de publicité programmatique à « la plus grande fuite des données »¹⁸.

Ces aspects ne font pas partie de notre recherche, bien que celle-ci soit ancrée en marketing : c'est pourquoi il nous paraît important d'intégrer ce sujet dans un futur agenda de recherche (cf. chapitre 7).

¹⁷ https://www.lemonde.fr/pixels/article/2022/01/20/l-utilisation-de-google-analytics-jugee-contraire-au-droit-europeen-sur-les-donnees-personnelles_6110287_4408996.html

¹⁸ Le Monde (16.05.2022) : Publicité programmatique : les données personnelles des internautes diffusées à leur insu plusieurs centaines de fois par jour (accessible à : <https://www.lemonde.fr/pixels/article/2022/05/16/publicite-programmatique-les-donnees-personnelles-des-internautes-diffusees-a-leur-insu-plusieurs-centaines-de-fois-par-jour>)

1.3. Diversité des violations de données personnelles

Les violations de données personnelles peuvent porter sur des données intimes et sensibles (e.g., état de santé ou orientation sexuelle) ou sur des données financières (e.g., numéro de carte bancaire). Nous avons fait le choix de considérer uniquement les violations de données qui ont un objectif de gain direct d'argent (excluant les cyberattaques politiques ou concurrentielles, même si dans ce cas aussi l'objectif lucratif est discutable). Dans cette partie, nous souhaitons illustrer cette définition des violations de données personnelles (e.g., intimes ou financières ; ancrées dans un objectif lucratif) avec plusieurs exemples significatifs.

1.3.1. *Scandales emblématiques de violations de données sensibles*

En 2015, le groupe de pirates informatiques The Impact Team publie les données de 37 millions d'utilisateurs du site de rencontres adultères et extraconjugales Ashley Madison (e.g., mails et préférences sexuelles), poussant jusqu'au suicide certains utilisateurs aux USA et au Canada¹⁹. Cette attaque était motivée par des criminels informatiques et cette opération leur a permis de gagner plusieurs millions de dollars²⁰. En 2018, le site de rencontres homosexuelles Grindr autorise des entreprises tierces à accéder aux données sensibles de ses utilisateurs, dont leur statut VIH²¹. Toujours en 2018, Facebook laisse Cambridge Analytica exploiter les données de plus de 87 millions d'utilisateurs, jouant un rôle majeur dans les élections américaines²². Malgré cela, Grindr et Facebook continuent à faire l'objet de piratages (e.g., en avril 2021, 533 millions de numéros de téléphone, d'adresses électroniques et d'informations biographiques d'utilisateurs de Facebook dans 106 pays ont été divulgués²³ ; Grindr a à nouveau été piraté début 2022²⁴) qui viennent continuellement s'immiscer dans le débat public et dont les objectifs peuvent être

¹⁹ New York Times (20.07.2015) : Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions (disponible à : <https://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html>)

²⁰ https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

²¹ Forbes (29.05.2018) : Report Says Grindr Exposed Millions Of Users' Private Data, Messages, Locations (disponible à : <https://www.forbes.com/sites/janetwburns/2018/03/29/report-says-grindr-exposed-millions-of-users-private-data-messages-locations/>)

²² New York Times (04.04.2018) : Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (disponible à : <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>)

²³ Insider (03.04.2021): 533 million Facebook users' phone numbers and personal data have been leaked online (disponible à : <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>)

²⁴ Wall Street Journal (02.05.2022) : Grindr User Data Was Sold Through Ad Network (disponible à : https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800?st=bc2b1sh63rcfhvr&reflink=desktopwebshare_permalink)

très variables. Toujours aux États-Unis en plein débat pour le droit à l'avortement, la filiale californienne de Planned Parenthood déclare une violation de données de 400.000 patientes, incluant leur géolocalisation et leur parcours de soins pour un avortement²⁵ : ces données pouvant être achetées pour 160\$. En France, en avril 2022, la société Dedalus est condamnée à 1,5 million d'euros d'amendes suite à la fuite mi-février 2021 de données médicales de 500 000 Français (e.g., nom, prénom, adresse postale, numéro de téléphone, e-mail, groupe sanguin, numéro de Sécurité sociale, informations relatives au statut médical, telles que VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux, données génétiques)²⁶. Dans ce contexte, les cyberattaques des établissements de santé sont de plus en plus fréquentes : nous les illustrons dans le paragraphe suivant.

1.3.2. Cyberattaques des établissements de santé et hospitaliers

Les cyberattaques de centres de santé et hospitaliers sont de plus en plus fréquentes : en 2021, en moyenne, un incident par semaine intervient dans une entité du secteur de la santé²⁷. En France, elles ont été médiatisées avec la cyberattaque du centre hospitalier de Corbeil-Essonnes fin août 2022. Les données médicales peuvent être revendues 250€ l'unité sur le darknet²⁸ dans deux buts : (i) du cyber espionnage à but politique ou industriel (e.g., connaître et/ou manipuler la viabilité de vaccins étrangers), (ii) de la falsification d'identité pour avoir accès à une couverture médicale, à des soins, à des médicaments²⁹. Pour y remédier, le gouvernement français débloque régulièrement des enveloppes budgétaires pour renforcer le niveau de cybersécurité des acteurs publics français : 136 millions d'euros en septembre 2020 dans le cadre du plan France Relance³⁰, 25 millions d'euros entre 2021 et 2022, 20 millions d'euros suite à la cyberattaque du centre de Corbeil-Essonnes³¹.

²⁵ New York Times (01.12.2021): Planned Parenthood Says Hacker Compromised Information for 400,000 Patients (disponible à: <https://www.nytimes.com/2021/12/01/us/planned-parenthood-data-breach-los-angeles.html>)

²⁶ <https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie>

²⁷ <https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/portraits-de-la-relance/centre-hospitalier-universitaire-de-reims/>

²⁸ <https://www.radiofrance.fr/franceculture/pourquoi-les-pirates-informatiques-ciblent-le-secteur-de-la-sante-9559739>

²⁹ <https://www.pialab.io/2021/04/27/donnees-de-sante-quel-interet-pour-les-pirates/>

³⁰ <https://www.economie.gouv.fr/plan-de-relance#>

³¹ [https://www.zdnet.fr/actualites/20-millions-d-euros-sur-la-table-pour-protger-les-hopitaux-des-cyberattaques-39946328.htm#:~:text=L'enveloppe%20des%2020%20millions,CHSF\)%20de%20Corbeil%2DEssonnes](https://www.zdnet.fr/actualites/20-millions-d-euros-sur-la-table-pour-protger-les-hopitaux-des-cyberattaques-39946328.htm#:~:text=L'enveloppe%20des%2020%20millions,CHSF)%20de%20Corbeil%2DEssonnes)

1.3.3. Exemples historiques de violations de données bancaires ou financières

De façon moins dramatique, mais tout aussi importante, les violations de données touchent également les données personnelles des clients de grandes entreprises. Un premier exemple notoire est celui de la chaîne américaine de magasins discount Target. L'entreprise a été victime d'une intrusion informatique ayant conduit au vol de plus de 40 millions de numéros de cartes de crédit en pleine période de Thanksgiving en 2013, alors que le groupe semblait bénéficier d'une bonne protection informatique. Les pirates se sont introduits dans le système par l'intermédiaire d'un sous-traitant de Target. Les données ont été trouvées en vente sur le marché noir informel. Le directeur général du groupe a démissionné, les pertes pour la chaîne ont été estimées à 1 milliard de dollars en chiffre d'affaires, les bénéfices de l'entreprise ont chuté de près de 50 % au quatrième trimestre de 2013, Target a réglé un recours collectif de 10 millions de dollars en 2015. En 2017, Target a payé 18,5 millions de dollars de plus en règlements³², sans compter l'impact de la fuite en termes de perte de réputation. La violation des données de Target a été l'une des plus grandes violations de sécurité de l'histoire : elle a servi de modèle pour de nombreux travaux conduits par le Sénat américain.

Un autre exemple est celui de l'agence de crédit américaine Equifax qui, en 2017, a signalé une violation affectant les données d'environ 147 millions de consommateurs américains (e.g., numéros de sécurité sociale, permis de conduire, numéros de cartes bancaires)³³, entraînant une pénalité imposée par la Federal Trade Commission (FTC) de 700 millions de dollars. En février 2021, l'agence mondiale d'évaluation de crédit Experian qui a fait état d'une fuite massive de données au Brésil de plus de 220 millions de citoyens, en raison d'activités illégales de sa filiale Court Ventures (e.g., consultation d'informations financières et de numéros de sécurité sociale de citoyens).

³² NBC News (24.05.2017) : Target Settles 2013 Hacked Customer Data Breach For \$18.5 Million (disponible à : <https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031>)

³³ Wired (Septembre 2017) : How 4 Chinese Hackers Allegedly Took Down Equifax (disponible à : <https://www.wired.com/story/equifax-hack-china/>)

1.3.4. *Principales victimes des violations de données : les consommateurs*

Les consommateurs sont particulièrement touchés par les violations de données personnelles : 80 % des violations de données concernent des informations personnelles de clients en 2020³⁴. Ces données consommateurs ont de la valeur et sont revendues par des data brokers et sur le marché informel. Les consommateurs font ensuite l'objet, au mieux de ciblage publicitaire non souhaité, au pire de vol d'identité ou de discrimination (Citron & Solove, 2021). Cependant, les recours en justice restent peu instruits (Citron & Solove, 2021; Romanosky et al., 2013) et les consommateurs très faiblement indemnisés. Par exemple, dans le cas de Target : « *Les poursuites intentées par les consommateurs pour cette violation ont été réglées pour une somme dérisoire – à peine 10 millions de dollars (...) La violation des données de Target a touché entre 70 et 110 millions de personnes, ce qui signifie que le recouvrement n'a représenté que quelques centimes par personne* » (Solove & Hartzog, 2022, p.8). Les consommateurs sont donc dans une situation de grande vulnérabilité.

1.4. Volume, tendances haussières et impacts financiers des violations de données personnelles

Nous pourrions prolonger l'inventaire des violations de données personnelles pendant longtemps tant elles sont nombreuses :

- En 2021, seulement 20% des entreprises ont déclaré ne pas avoir été attaquées (vs. 32% en 2020³⁵) ;
- Entre janvier et novembre 2021, 952,8 millions de personnes ont été victimes d'une violation de données personnelles dans le monde, soit une personne sur 5³⁶ ;
- Aux États-Unis le nombre d'actes de violation de données est passé de 656 violations de données à 1.257 entre 2008 et 2018, impliquant 35,7 millions de données vs. 471,23 millions³⁷.

³⁴ IBM Cost of Data breach Report (disponible à : <https://www.ibm.com/security/data-breach>)

³⁵ Acronis Cyberthreats Report 2022 (disponible à : <https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/>)

³⁶ <https://www.lebigdata.fr/violation-de-donnees-2021>

³⁷ Statista : <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

Ces chiffres sous-estiment le nombre de violations qui ne sont pas toujours signalées par les entreprises. Nous verrons notamment dans la seconde partie de ce premier chapitre (portant sur les réglementations pour la protection des données personnelles) les procédures qui s'imposent en cas de violations de données personnelles. De plus, cette tendance s'est accentuée récemment par l'essor de la digitalisation de nos vies personnelles et économiques :

- Les volumes de stockage de données des systèmes informatiques mondiaux seront multipliés par 5,3 entre 2018 et 2025³⁸ ;
- La pandémie du Covid-19 ayant accéléré depuis 2020 la transformation digitale de la société et des entreprises, en particulier à travers le télétravail et l'enseignement en ligne, le risque d'exfiltration et d'exposition de données personnelles augmente ;
- Cette tendance va encore s'accroître avec l'essor des objets connectés (e.g., Apple Watch ou Alexa), des applications médicales (e.g., Doctolib) et de quantification de soi. Par conséquent, la question pour toute entreprise n'est alors plus de savoir si elle va être attaquée, mais quand elle va être attaquée.

Par ailleurs, ce sont les États-Unis qui sont les plus touchés, avec 214,4 millions de violations de bases de données signalées en 2021³⁹, suivi de l'Allemagne et du Canada⁴⁰.

Enfin, le coût des violations de données est colossal. En 2020, le coût total moyen d'une violation de données dans les entreprises de plus de 25.000 employés est de 5,52 millions de dollars (vs. 2,64 millions de dollars pour les organisations de moins de 500 employés), et est de 7,13 millions de dollars dans le secteur de la santé (+10 % vs. 2019). Une violation de données coûte 3,86 millions de dollars en moyenne et une donnée personnelle violée génère un coût moyen de 150\$⁴¹.

³⁸ Étude Data Age 2025, IDC, 2018. *op. cit.*

³⁹ <https://www.lebigdata.fr/violation-de-donnees-2021>

⁴⁰ Acronis Cyberthreats Report 2022. *op. cit.*

⁴¹ IBM Cost of Data breach Report. *op. cit.*

1.5. Cybercriminalité et moyens mis en œuvre face aux violations de données personnelles : le « far-west »

Les violations de données personnelles relèvent essentiellement de la cybercriminalité. En effet, les experts observent une forte augmentation du nombre d'incidents de sécurité informatique, dont **près d'un quart sont des violations de données et environ 4 violations sur 5 sont attribuées à des actions criminelles**⁴². Parmi ces actes criminels, les *ransomwares* (i.e., demandes immédiates de rançons pour récupérer des données personnelles et des logiciels après prise de contrôle à distance d'un système) sont les plus fréquents et en augmentation de 13% en 2021⁴³. Ainsi, les *ransomwares* sont la principale menace pour les grandes et moyennes entreprises, les administrations publiques, les services de santé et d'autres organisations critiques⁴⁴.

Ce contexte est un véritable *far-west*, avec ses shérifs, ses chasseurs de primes et ses justiciers :

- Cette criminalité et ces actions de *ransomware* amènent à des actions policières de très grande envergure, plaçant principalement plusieurs grands acteurs comme Interpol/Europol comme les shérifs de notre *far-west* des violations de données personnelles. En 2021, Europol, la Gendarmerie nationale française, la Police nationale ukrainienne et le Federal Bureau of Investigation des États-Unis ont arrêté deux opérateurs de ransomware responsables de l'extorsion de 70 millions d'euros. 375.000 dollars américains en espèces, deux voitures de luxe et 1,3 million de dollars américains en cryptomonnaie ont également été saisis⁴⁵ ;
- Des primes peuvent être proposées pour attraper les pirates informatiques. Aux États-Unis en 2021, un programme de récompense a été lancé : une prime de 10 millions de dollars pour chacun des membres de REvil (Sodinokibi) et Darkside ransomware dénoncé⁴⁶;

⁴² Verizon 2022 Data Breach Investigations Report (disponible à : <https://www.verizon.com/business/resources/reports/dbir/>)

⁴³ Verizon 2022 Data Breach Investigations Report. *op. in.*

⁴⁴ Acronis Cyberthreats Report 2022. *op. cit.*

⁴⁵ L'Usine Digitale (04.10.2021) : Les polices française, américaine et ukrainienne arrêtent deux opérateurs de ransomwares (accessible à : <https://www.usine-digitale.fr/article/les-polices-francaise-americaine-et-ukrainienne-arretent-deux-operateurs-de-ransomwares.N1146942>)

⁴⁶ <https://www.zdnet.fr/actualites/ransomware-une-prime-de-10-millions-de-dollars-pour-des-informations-sur-darkside-39931951.htm>

- Enfin, comme dans tout *far-west*, nous avons également des justiciers qui conduisent des actions de piratage pour défendre le bien commun. Le plus connu est Edward Snowden⁴⁷, qui a révélé en juin 2013 des milliers de documents classifiés de la NSA à différents journalistes internationaux, dévoilant ainsi des programmes de surveillance et d'écoute mondiaux. Plus récemment en mai 2022, une enquête menée par Adrian Zenz (universitaire allemand) et 14 médias internationaux a confirmé la déportation des Ouïghours à l'aide de données piratées par un inconnu sur des ordinateurs de la police du Xinjiang (<https://www.xinjiangpolicefiles.org/>)⁴⁸. Ce point étant éloigné de notre sujet, nous ne l'approfondirons pas.

1.6. Cybersécurité, sécurité informatique et protection des données personnelles

Dans ce contexte, de nombreuses réglementations sont mises en place : en sécurité informatique, en cybersécurité et en sécurité de l'information. Elles se différencient ainsi :

- La sécurité informatique s'occupe de tous les éléments informatiques permettant de stocker des informations numériques (systèmes, réseaux informatiques, matériels, logiciels) dans l'objectif de protéger l'intégrité des technologies de l'information ;
- La cybersécurité traite des menaces qui peuvent exister dans le cyberspace et s'occupe de l'approche générale adoptée par une organisation pour protéger ses réseaux, ses dispositifs et ses données contre les menaces du cyberspace (e.g. contrôles d'accès réseau, configurations des matériels, pare-feu) ;
- La sécurité de l'information qui s'occupe de la protection des actifs d'information, de leur intégrité, de leur confidentialité et de leur disponibilité (e.g., modèle SAPAS d'Acronis pour Safety, Accessibility, Privacy, Authenticity, Security).

La sécurité de l'information comprend le respect des réglementations de conformité en vigueur, telles que le RGPD, la norme de sécurité des données du secteur des cartes de paiement (PCI

⁴⁷ The Guardian (11.06.2013) : Edward Snowden: the whistleblower behind the NSA surveillance revelations (disponible à : <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>)

⁴⁸ Le Monde (24.05.2022) : 'Xinjiang Police Files': Exclusive documents reveal China's machine of repression against the Uyghurs (disponible à : https://www.lemonde.fr/en/international/article/2022/05/24/xinjiang-police-files-exclusive-documents-reveal-china-s-machine-of-repression-against-the-uyghurs_5984537_4.html)

DSS), la loi sur la portabilité et la responsabilité de l'assurance maladie (HIPAA), la loi fédérale de 2002 sur la gestion de la sécurité de l'information (FISMA), la loi sur les droits à l'éducation familiale et à la vie privée (FERPA).

La protection des données personnelles fait partie de la sécurité de l'information : « *la sécurité peut être considérée comme l'une des conditions requises pour garantir le respect de la vie privée* » (Beke et al., 2018, p.6).

En conclusion : sans sécurité, pas de vie privée ! Cet adage guide toute notre recherche, notre positionnement ainsi que l'ambition de cette thèse.

*

Nous venons de définir les données personnelles (i.e., toute information confidentielle permettant d'identifier une personne) et les violations de données personnelles (i.e., tout vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif). Des procédures de sécurité informatique, incluant le respect des réglementations pour la protection des données personnelles, dont le RGPD, sont établies pour se protéger des violations de données : car sans sécurité, pas de vie privée. Nous allons désormais préciser dans la partie suivante les réglementations existantes.

2. Réglementations pour la protection des données personnelles

Dans cette partie, nous exposons l'histoire de la protection de la vie privée et de la mise en place de réglementations internationales en la matière (2.1.). Nous détaillons le RGPD (2.2.) (en précisant les procédures à suivre en cas de violations de données personnelles), et les autres réglementations internationales (2.3.). Enfin, nous faisons état des variations observées au sein de l'Europe dans l'adoption du RGPD (2.4.).

2.1. Histoire de la protection de la vie privée

2.1.1. Définition d'un droit fondamental universel à la vie privée

Les réglementations pour la protection des données personnelles qui apparaissent dans le monde reposent sur le concept de « protection de la vie privée » qui est assez récent. En effet, si le souhait de distinguer les sphères privée et publique de sa vie existe depuis toujours (Ariès & Duby, 1985), le concept de « protection de la vie privée » s'est développé avec le développement des supports de communication (images ou télécommunications) à la fin du XIX^{ème} siècle. La protection de la vie privée a été définie juridiquement pour la première fois aux États-Unis par le juge Cooley comme le « droit d'être laissé seul » (*right to be let alone*), à une époque où les photographies commençaient à circuler de plus en plus aux États-Unis (Warren & Brandeis, 1890). À cette même époque, Warren & Brandeis (1890) considéraient que la protection de la vie privée était absolument essentielle dans le développement de nos sociétés, car elles reposaient principalement sur les communications.

Le droit à la vie privée, distingué de la liberté d'expression, d'association et de croyance, est un droit fondamental affirmé par la Déclaration universelle des droits de l'homme (adoptée par les Nations unies en 1948) dans son article 12 : « ***Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes*** ». La Déclaration universelle des droits de l'homme de 1948 vise à protéger les individus des excès de la Seconde Guerre mondiale et, en particulier, en ce qui concerne les droits de protection de la vie privée : tels que le fichage des personnes, l'ingérence de la police dans le domicile des personnes, et la possibilité d'identifier des relations spécifiques, des préférences sexuelles ou des convictions politiques. Pour mémoire, la société

Dehomag (Deutsche Hollenrith-Maschinen Gesellschaft), à cette époque filiale d'IBM, avait notamment permis d'identifier les juifs durant les années 30, ce qui facilita leur déportation dans les camps de concentration. Par ailleurs, la Déclaration universelle des droits de l'homme de 1948 réaffirme l'esprit du siècle des Lumières qui, d'une part, exige la transparence contre « *l'arbitraire politique, les caprices des monarques, les superstitions religieuses, les complots des tyrans et des prêtres, les illusions de l'ignorance, les épidémies* » (Foucault, 2001, p.197) et, d'autre part, un droit à la vie privée comme clé de voûte de la démocratie, sans lequel les gens sont sous surveillance constante et perdraient donc leur liberté (Sykes, 1999).

Ainsi, le droit à la vie privée est une protection générale contre toute intervention arbitraire (en particulier une protection contre l'entrée d'autrui dans un domicile privé) ou toute interférence arbitraire dans la vie privée professionnelle et médicale, dans les affaires intimes d'une personne (e.g., relations et préférences sexuelles), en particulier l'utilisation d'images, les écoutes téléphoniques et l'accès aux données personnelles.

Par la suite, ce droit fondamental à la vie privée a été adopté dans différentes lois, comme la Convention européenne des droits de l'homme de 1953 (article 8) ou le Code civil français de 1970 (article 9). En particulier, le droit à la vie privée, en vertu de l'article 8 de la Convention européenne des droits de l'homme, a été utilisé principalement dans des affaires concernant les LGBT (*Lesbian, Gay, Bisexual, Transgender*), comme l'affaire Smith et Grady au Royaume-Uni (Privacy Law Library, 1999⁴⁹), dans laquelle un membre de la Royal Navy avait été exclu de son service en raison de son orientation sexuelle.

Afin de ne pas perdre de vue la finalité des réglementations en matière de vie privée, qui se fondent sur un impératif de sécurité, nous retraçons dans la Figure 3 (page suivante) l'historique de la construction du droit à la vie privée. Nous souhaitons par là même insister sur l'objectif sécuritaire d'une protection à la vie privée, et du lien entre vie privée et sécurité.

⁴⁹ Privacy Law Library (1999), accessible à : <https://privacylibrary.ccnlud.org/case/smith-and-grady-vs-the-united-kingdom>

2.1.2. *Développement de la protection de la vie privée dans les années 1980*

À partir de la fin des années 1970, avec le développement de l'informatique, la problématique a pris de l'ampleur et de nouvelles réglementations ont été mises en place, notamment en France, en Allemagne, au Royaume-Uni et aux États-Unis. En France, la CNIL a été créée en 1978 en parallèle de la Loi Informatique et Libertés, suite à l'affaire Safari (SAFARI = Système Automatisé pour les Fichiers Administratifs et Répertoires des Individus), i.e., un projet de l'État français qui visait à mettre en place un grand fichier unique des citoyens français, et qui a fait l'objet de très fortes contestations (les souvenirs de la Seconde Guerre mondiale étant encore récents). Ainsi, la réglementation de la vie privée en France a été établie pour empêcher la surveillance de l'État.

De même, l'Australie a souhaité instaurer en 1985 une carte nationale d'identité (« Australia Card ») pour lutter contre la fraude fiscale et le détournement d'usage des aides sociales. Cette initiative a soulevé un très fort mouvement de contestations au sein de la population australienne, qui a abouti à un compromis avec, d'une part, la création d'un système de numéros de dossier fiscal (écartant donc la question des aides sociales) et, d'autre part, l'adoption d'un premier texte législatif en matière de protection de la vie privée, le Privacy Act de 1988 (Greenleaf, 2008).

2.1.3. *Mise en place de réglementations spécifiques dans les années 1990*

Dans les années 90, des dispositions relatives à la protection des données personnelles limitées à un secteur d'activités, à une catégorie de population ou à un type de données ont été instaurées : par exemple aux États-Unis, le « Health Insurance Portability and Accountability Act » (HIPAA) en 1996 pour le secteur de la santé et le « Children's Online Privacy Protection Act » (COPPA) en 1998 pour la protection de la vie privée des mineurs de moins de 13 ans.

2.1.4. *Développement des réglementations pour la protection des données personnelles dans les années 2000*

À partir de la fin des années 1990, nous observons un double phénomène : la mise en place de nouvelles réglementations pour la protection des données personnelles dans différents pays et le lancement des travaux préparatoires au RGPD. Ces deux phénomènes sont liés.

Pour exemple, le Protection and Electronic Documents Act (PEDA) entré en vigueur en 2000 au Canada vise à rassurer l'Union européenne sur la capacité de la loi canadienne sur la protection de la vie privée à protéger les informations personnelles des citoyens européens. De même, la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) a été créée le 18 février 2009 au Maroc. Le développement de ces réglementations répond essentiellement à des nécessités économiques (e.g., maintien d'activités d'offshoring au Maroc ; besoin qui est encore plus important face à une réglementation extraterritoriale comme le RGPD).

Depuis lors, et parce qu'elle est également une référence en matière de protection des droits de l'homme, l'Europe est une référence en matière de protection de la vie privée et des données personnelles (Greenleaf, 2012).

Les instances européennes ont donc travaillé au renforcement des droits des utilisateurs et à l'harmonisation des réglementations au sein de l'Europe, essentiellement celles issues des trois autorités nationales fondatrices : la CNIL en France, l'ICO (*Information Commissioner's Office*) au Royaume-Uni, ou le BND (*Bundesnachrichtendienst*) en Allemagne. Les travaux de réforme de la législation concernant la protection des données ont été lancés en 1995. Un nouveau règlement portant sur un ensemble de règles uniques pour toutes les données collectées pour l'ensemble des résidents de l'Union européenne a été proposé en 2012. Les négociations entre le Parlement, le Conseil et la Commission ont débuté en juin 2015 pour aboutir à un accord de principe le 15 décembre 2015. Le Parlement a donné son accord en avril 2016 et le RGPD est entré en vigueur le 25 mai 2018 dans toute l'Europe.

Nous précisons dans les paragraphes suivants les principes et effets du RGPD.

Figure 3 : Principales étapes de l'histoire de la protection de la vie privée

Année	Contexte	Texte
1890	Développement des supports de communication	Juge Cooley aux USA : « <i>right to be left alone</i> »
Années 30	Montée du nazisme en Allemagne	Collaboration de la société Dehomag (filiale IBM) pour identification des juifs
1948	Déclaration universelle des droits de l'homme	Article 12 : instauration d'un droit à la vie privée (protégeant de toute immixtions arbitraires)
1953	Convention européenne des droits de l'homme	Article 8 : intégration du droit à la vie privée
1970	Code civil français	Article 9 : intégration du droit à la vie privée
1978	Affaire SAFARI en France	Création de la CNIL et de la loi Informatique & Libertés (objectif : empêcher surveillance de l'Etat)
1988	Affaire Australia Card	Privacy Act en Australie (objectif : empêcher surveillance de l'Etat)
1994	Affaire Smith & Grady	Un membre de la Royal Navy est exclu de son service en raison de son orientation sexuelle
Entre 1995 et 2005	Montée en puissance des réglementations	HIPAA (1996) et COPPA (1998) aux Etats Unis ; PEDPA (2000) au Canada ; CNDP (2009) au Maroc
2018	Affaire Smith & Grady	Entrée en vigueur du RGPD en Europe

Nota bene : le graphe ci-dessus ne se veut pas exhaustif. De plus, y figurent des grandes décisions légales (entourées en vert), des décisions moins impactantes (entourées en trait plein) et des exemples ayant permis de faire évoluer les législations (entourés en pointillés).

2.2. Règlement Général pour la Protection des Données personnelles

2.2.1. Principes du RGPD

Le RGPD a pour objectif principal de protéger le droit des citoyens de décider de la protection de leurs données personnelles. Le RGPD (comme la majorité des réglementations internationales) repose sur le principe du droit des citoyens de décider avec qui et de quelle manière ils souhaitent partager leurs données. Ce principe, appelé également *self-data management*, est à la base des notions de consentement et de droit de retrait et d'effacement des données. Le principe de self-data management implique une responsabilité des individus dans la gestion de leurs données. Si celui-ci est efficace dans un contexte de sollicitation relativement contrôlée des données personnelles, il peut être remis en question dans un contexte de digitalisation accrue et d'insécurité informatique (Solove, 2020).

Les entreprises sont tenues dans le cadre du RGPD de ne collecter que les données personnelles nécessaires et d'être transparentes dans leurs pratiques. Elles se doivent de sécuriser les données (informatiquement et physiquement) et de penser aux droits des personnes (droits d'accès, de rectification et de suppression des données personnelles).

En somme, les 8 règles d'or du RGPD sont les suivantes :

- Licéité du traitement (e.g., obligation d'obtenir le consentement des personnes, réalisation d'un traitement des données uniquement si nécessaire au regard d'une obligation contractuelle et/ou légale) ;
- Finalité du traitement précise et légitime ;
- Minimisation des données (i.e., traitement des données strictement nécessaires) ;
- Protection particulière des données sensibles ;
- Conservation limitée des données ;
- Obligations de sécurité ;
- Transparence (socle du contrat de confiance qui personnes et organisations) ;
- Droits des personnes (i.e., les personnes bénéficient de droits leur permettant de garder la maîtrise de leurs données).

2.2.2. *Obligations et possibilités instaurées par le RGPD en cas de violations de données personnelles*

Le RGPD impose des obligations légales importantes aux entreprises, telles que : (i) signaler tout cas de violation de données personnelles, (ii) nommer un Délégué à la Protection des Données (Data Protection Officer - DPO), (iii) obtenir le consentement des personnes concernées pour collecter leurs données. Les organismes qui traitent des données personnelles doivent non seulement mettre en place des mesures pour prévenir les violations de leurs données, mais également (Art. 33 et 34 du RGPD) notifier toute violation de données en informant la personne dont les données personnelles ont été violées (cf. exemple de notification en Annexe 1).

Le non-respect de ces principes entraîne des sanctions et des amendes, qui peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires. De plus, les sanctions pénales peuvent être appliquées allant de 5 ans d'emprisonnement et 300.000 d'euros d'amende pour une personne physique, et jusqu'à 1,5 million d'euros d'amende pour une personne morale (Art. 226 du Code pénal).

Par ailleurs, toute personne a la possibilité de porter plainte auprès du régulateur (e.g., CNIL) si elle constate une atteinte aux règles de protection des données personnelles par un organisme public ou privé et souhaite le signaler.

La question demeure : ces obligations et possibilités sont-elles efficaces et suffisantes face à un nombre accru de violations de données personnelles ?

2.2.3. *Effets du RGPD sur les pratiques et les violations de données*

Le RGPD a généré une augmentation de la sensibilité à la protection des données personnelles et des bonnes pratiques. Il a également permis de soutenir des décisions comme l'interdiction de Google Analytics (l'outil d'analyse de tracking web le plus utilisé) par plusieurs autorités de protection des données personnelles en Europe pour cause de non-conformité au RGPD, car il transfère des données personnelles aux États-Unis (ce qui est interdit depuis l'interdiction du Privacy Shield et l'arrêt Schrems II en juillet 2020).

Les effets restent cependant plus contrastés et confus sur le marché publicitaire. L'interdiction des cookies tiers reste lente. Google a abandonné le projet de ciblage FLoC⁵⁰, a finalement reporté à 2024 l'élimination progressive des cookies tiers dans Google Chrome⁵¹. Apple, qui a cherché à marquer la différence avec l'Android de Google en lançant l'App Tracking Transparency (qui consiste à obliger les applications à vous demander la permission avant de vous suivre sur iPhone) et en communiquant sur des règles de confidentialité très strictes, a été fortement remis en question⁵². De plus, le RGPD a eu pour conséquence de favoriser la concentration de fournisseurs offrant des services d'assistance aux sites web, enregistrant une baisse du nombre de sociétés de 15% (Johnson et al., 2022).

De même, les effets du RGPD sur les violations de données sont contrastés. Certaines recherches montrent un effet bénéfique des réglementations sur le nombre de violations de données personnelles (e.g., évaluation d'une baisse de 6% des vols d'identité liés à des violations de données sur la base d'un panel de la FTC ; Romanosky et al., 2013). Mais, cette recherche est ancienne. La société Acronis⁵³ prédit que la prolifération des réglementations sur la confidentialité des données ne ralentira pas les faits signalés de violations de données personnelles. En effet, les systèmes informatiques se complexifient et les entreprises ont de plus en plus de difficultés à retracer tous les échanges. Les objets connectés et les connexions M2M

⁵⁰ FLoC (Federated Learning of Cohorts Explained Flock) consiste à regrouper les utilisateurs partageant les mêmes centres d'intérêt dans des segments d'audience pour éviter tout risque d'identification univoque. Mais ces segments, ou cohortes, étant d'une centaine d'utilisateurs, ils ne permettent pas de se prémunir de tout risque de ré-identification des individus, notamment avec des techniques de fingerprinting, i.e., approche probabiliste de comparaison d'empreintes digitales (The New York Times, 2021).

⁵¹ Bloomberg (27.07.2022). Google Delays Phasing Out Ad Cookies on Chrome Until 2024, disponible à : <https://www.bloomberg.com/news/articles/2022-07-27/google-delays-phasing-out-ad-cookies-on-chrome-until-2024>

⁵² Financial Times (2021) Apple reaches quiet truce over iPhone privacy changes. Disponible à : <https://www.ft.com/content/69396795-f6e1-4624-95d8-121e4e5d7839>.

⁵³ Acronis Cyberthreats Report 2022. *op. cit.*

(*machine-to-machine*, i.e., toutes les informations échangées dans le cadre des communications entre machines) génèrent une augmentation très forte des échanges de données. Cette complexité facilite les attaques informatiques.

Par conséquent, le RGPD ne suffit pas à juguler les violations de données personnelles et à totalement protéger les individus. Pour cela, il est impératif d'éduquer les personnes aux enjeux de cybersécurité et à leur faire adopter les bons comportements (Weber & Jean-Philippe, 2017). Mais pour changer les comportements, il faut les comprendre : voici toute l'ambition de notre recherche.

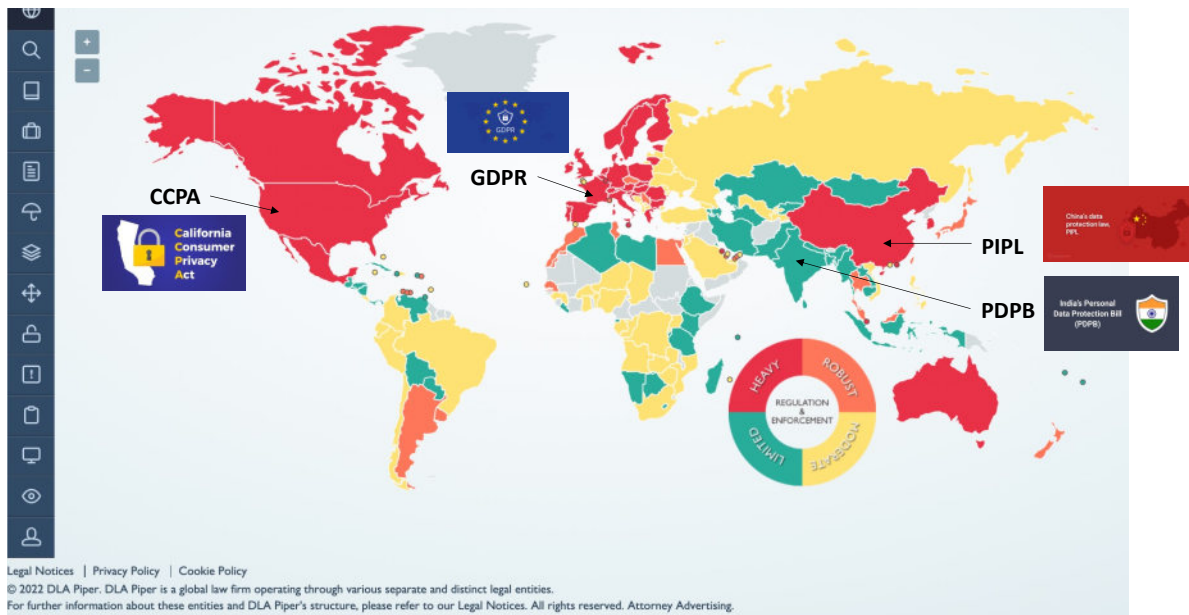
Enfin, malgré le souhait d'harmoniser les réglementations européennes, de grandes disparités au sein de l'Europe sont constatées.

2.3. Réglementations internationales pour la protection des données personnelles en vigueur

Si le RGPD est considéré comme un système juridique de référence en matière de protection des données, d'autres réglementations ont été mises en place à travers le Monde et une récente étude indique que les lois sur la protection des données personnelles s'appliqueront à 75% des consommateurs à travers le monde d'ici 2024⁵⁴. La carte présente dans la Figure 4 suivante fait état des réglementations internationales de protection de données personnelles : cette carte est évolutive au fur et à mesure de l'entrée en vigueur de nouvelles réglementations.

⁵⁴ <https://iapp.org/news/a/gartner-predicts-75-of-consumers-will-fall-under-privacy-laws-by-2023/>

Figure 4 : Carte des législations internationales de protection de données personnelles⁵⁵



Quatre réglementations sont précisées sur la carte qui précède :

- RGPD (GDPR en anglais) ;
- CCPA, California Consumer Privacy Act, entrée en vigueur en septembre 2018 (peu de temps après le RGPD), devenue en novembre 2020 le CPRA, California Privacy Right Act, renforçant les droits des consommateurs à contrôler l'usage de leurs données personnelles (e.g., droit de correction, droit de limiter l'usage des données) ;
- Le PDPB, India's Personal Data Protection Bill, entré en vigueur en décembre 2019. Ce règlement est intéressant à suivre car (i) il s'applique à une population de 1,4 milliard de personnes, (ii) il vise un niveau de protection proche du RGPD, (iii) l'Inde avait surpris en 2016 en refusant l'offre d'Internet gratuit Free Basics de Facebook (avec des manifestations citoyennes importantes pour défendre la neutralité du web) ;
- Le PIPL, Personal Information Protection Law, entré en vigueur en Chine en novembre 2021. Ce règlement pose des questions de compatibilité avec des pratiques en cours comme la vidéo surveillance de masse ou le crédit social (i.e., un capital de points est accordé par l'État au citoyen selon un comportement surveillé).

Dans le Tableau 3 page suivante, cinq blocs de pays sont identifiés selon le niveau de conformité de leur législation en matière de protection de données personnelles avec le RGPD (totalement

⁵⁵ Carte DLA Piper Global Data protection laws of the world, disponible à : <https://www.dlapiperdataprotection.com/>

conforme, partiellement conforme, existence d'une législation reconnue par la Conférence internationale des commissaires à la protection de la vie privée et des protecteurs des données personnelles, existence d'une législation non reconnue, aucune législation). Ce tableau a été établi par la CNIL (2022⁵⁶). Il est également évolutif.

Tableau 3 : Législations internationales en matière de protection de données personnelles et degrés de conformité avec le RGPD

Bloc	Législation et niveau de conformité		États (exemples)
# 1	Pays en totale adéquation	- RGPD appliqué ou réglementation en totale adéquation	Europe (28 pays membres) Royaume-Uni Suisse Japan Argentina and Uruguay
# 2	Pays partiellement en adéquation	- Adéquation au RGPD pour les entreprises qui ont adhéré à la loi en vigueur - Traitements spécifiques nécessaires pour les autres	Canada (PIPEDA: Personal Information Protection and Electronic Documents Act)
# 3	Pays disposant d'une autorité régulatrice et d'une législation	- Existence d'une législation nationale sur la protection des données et d'une autorité de protection des données reconnue par la Conférence internationale des commissaires à la vie privée et des protecteurs des données personnelles. - Les transferts de données personnelles vers ces pays nécessitent des outils de transfert.	États-Unis (Privacy Shield) Afrique du Sud Australie (OAIC : Office of the Australian Information Commissioner) Mexique (INAI : El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) Maroc (CNDP : Commission Nationale de contrôle de la protection des Données à caractère Personnel) Sénégal (CDP : Commission de Protection des Données Personnelles) Côte d'Ivoire (ARTCI : Autorité de Régulation des Télécommunications) Ghana (Data Protection) Ukraine
# 4.	Avec une législation	- Pays non reconnu comme adéquat par l'Union européenne. - Le transfert de données personnelles vers ces pays nécessite des outils de transfert.	Russie Chine (PIPL : Personal Information Protection Law) Inde (Data Protection Bill) Brésil (LGPD : Lei Geral de Proteção de Dados)
# 5.	Absence de législation		Bolivie

⁵⁶ <https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde>

2.4. Variabilité dans la mise en œuvre des réglementations pour la protection des données personnelles

2.4.1. Variabilité internationale dans l'interprétation du droit à la vie privée

La vie privée est un concept très subjectif, qui varie selon l'époque, le pays ou l'individu (Ariès & Duby, 1985). Pour exemple, l'indicateur de vie privée « Privacy Score » établi par BestVPN.org⁵⁷ expose des écarts importants entre les trois premiers pays du classement (Norvège, Australie, Danemark, soit des scores respectivement de 90,1%, 89,1% et 87,4%) et les trois derniers pays (Cambodge, Ouzbékistan, Chine, soit des scores respectivement de 15,6%, 15,0% et 13,1%).

Ceci a des conséquences directes sur les réglementations en vigueur. Par exemple, la loi américaine sur la vie privée vise l'équilibre entre intérêts privés et commerciaux afin de protéger le consommateur, alors que l'Union européenne considère le respect de la vie privée comme un droit fondamental des citoyens, supérieur à tout autre. Aux États-Unis, et malgré l'injonction de Warren & Brandeis (1890), « *un droit constitutionnel autonome à la vie privée n'existe pas* » (Martin & Murphy, 2017, p.137). Seuls des amendements intégrés à la United States Bill of Rights, en particulier le quatrième amendement, remettent en cause le droit des gouvernements à intervenir dans les affaires privées. La protection des données personnelles est du ressort de la FTC, qui utilise des leviers tels que les Fair Information Practices Principles (Ohlhausen, 2014). Quelques lois (citées précédemment) ont été adoptées aux États-Unis, comme le Children's Online Privacy Protection Act (1998). De plus, ces droits en matière de protection des données sont essentiellement axés sur la protection du consommateur. Ils sont gérés aux États-Unis par la FTC vs. la Commission européenne en Europe. La loi californienne entrée en vigueur en 2018 porte sur la protection des consommateurs (California Consumer Privacy Act, CCPA, 2018, devenu CPRA en novembre 2020) quand le RGPD en Europe ne mentionne pas le terme « consommateur ».

Cette variabilité internationale présente des risques d'écueil en matière de coopération internationale sur la protection des données personnelles. Pour exemple, la Cour de Justice européenne a invalidé en juillet 2020 le Privacy Shield, i.e., le régime de transferts de données

⁵⁷ <https://bestvpn.org/privacy-index/>. Ce score intègre plusieurs indicateurs par pays : taux d'utilisation d'internet, indice de confidentialité sur Internet, législation sur la cybercriminalité, législation sur la protection des données

personnelles entre l'Union européenne et les États-Unis. Cette décision est appelée « Shrems II » car elle a été instruite suite aux actions de l'activiste Max Shrems. Cette décision implique que les données des citoyens européens ne peuvent plus être hébergées aux États-Unis, avec de lourdes conséquences pour de nombreuses activités. Le 25 mars 2022, la présidente de la Commission européenne, Ursula von der Leyen, et le président des États-Unis, Joe Biden, ont annoncé un accord de principe sur un nouveau système de partage des données entre l'UE et les États-Unis, appelé Privacy Shields 2.0. Cet accord devrait bientôt entrer en vigueur, malgré les contestations fortes de plusieurs activistes.

2.4.2. *Variabilité entre pays européens dans l'adoption du RGPD*

Le RGPD est une réglementation européenne qui est appliquée à l'ensemble des citoyens européens, qui ont les mêmes droits et les mêmes devoirs. De plus, chaque pays européen a mis en place une autorité administrative nationale de protection des données personnelles (e.g., CNIL en France) qui est garante du bon respect du règlement sur le territoire national (cf. Annexe 3 : Ensemble des Data Protection Authorities (DPA) en Europe).

Cependant, des variations dans l'adoption et la mise en place du règlement sont constatées. Cela se traduit de trois manières : (i) dans les moyens dont dispose chaque autorité nationale, (ii) dans le montant des amendes appliquées par chaque pays, (iii) dans le nombre de plaintes déposées par les citoyens auprès des autorités administratives.

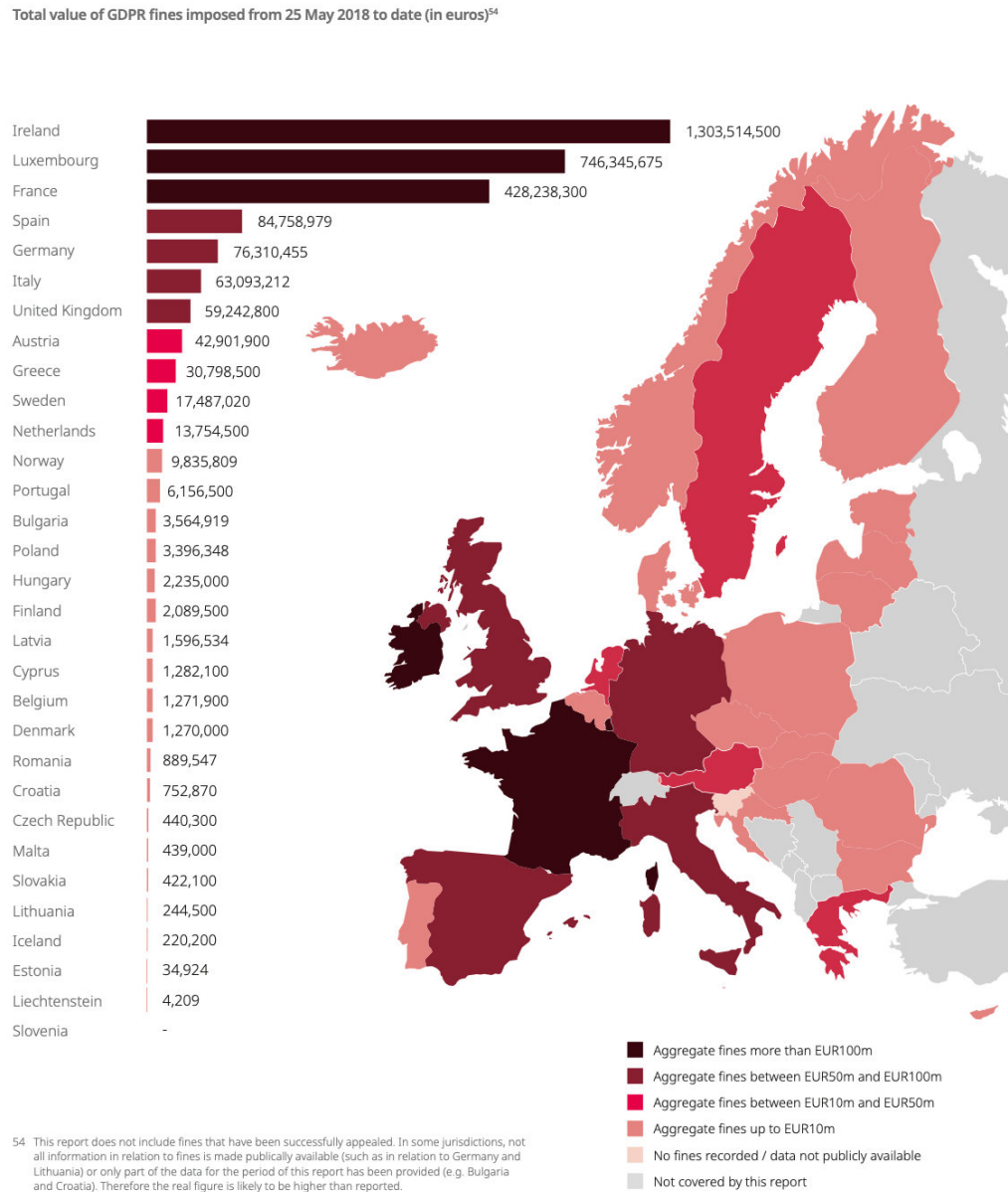
La Commission européenne reconnaît aussi que si la plupart des autorités ont vu leurs effectifs et budgets augmenter entre 2016 et 2019 (principalement en Irlande, Pays-Bas, Islande, Luxembourg et Finlande)⁵⁸, « *la situation reste toutefois inégale d'un État membre à l'autre et n'est pas encore globalement satisfaisante* » (p.7).

En outre, les autorités peuvent appliquer des sanctions aux entreprises en cas de non-respect des obligations liées au RGPD. Comme indiqué précédemment, les sanctions peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires. Les pays qui ont appliqué le montant total de sanctions le plus important sont le Luxembourg, l'Irlande, l'Italie et l'Allemagne selon les

⁵⁸ Communication de la commission au parlement européen sur la protection des données (disponible le 29 juillet 2022 à : <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0115:FIN:EN:PDF>)

enquêtes DLA Piper GDPR fines and data breach survey⁵⁹ (cf. Figure 5 ci-dessous). Les écarts sont surprenants : l'Italie a, par exemple, imposé un montant total de sanctions de près de 80 milliards d'euros sur la période, contre un peu plus de 880.000 € pour le Danemark.

Figure 5 : Valeur totale des amendes imposées dans le cadre du RGPD par chaque autorité nationale de protection des données personnelles (en € entre le 25 mai 2018 et le 27 janvier 2023)⁶⁰



⁵⁹ DLA Piper GDPR fines and data breach survey. *op. cit.*

⁶⁰ DLA Piper GDPR fines and data breach survey. *op. cit.*

Enfin, nous observons une très grande variabilité dans le nombre de plaintes pour violations de données personnelles déposées par les citoyens auprès des autorités nationales de protection de données personnelles⁶¹. Entre janvier 2022 et janvier 2023, les autorités administratives pour la protection des données personnelles ont enregistré aux Pays-Bas 142 plaintes pour 100.000 personnes pour violations de données personnelles, contre 133 au Danemark, 25 en Allemagne, 10 en Belgique, 8 en France, 3 en Italie, soit un rapport de 1 à 18 entre la France et les Pays-Bas. Ce rapport et le classement entre pays restent stables depuis 2018. Le détail du nombre de plaintes est présenté dans le Tableau 32. Ce sont ces données que nous utilisons dans le cadre de notre premier essai.

Cette variabilité nous amène à nous interroger sur le rôle des effets culturels dans les comportements d'adoption des réglementations pour la protection des données personnelles et, de façon plus large, sur l'influence de la culture sur les comportements de réponse face à une violation de données personnelles.

⁶¹ DLA Piper GDPR fines and data breach survey. *op. cit.*

Synthèse de la section sur le contexte managérial

Dans cette première section, nous avons apporté les définitions qui seront suivies dans cette thèse concernant les données personnelles (i.e., toute information confidentielle permettant d'identifier une personne) et les violations de données personnelles (i.e., tout vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif). Nous avons éclairé ces définitions à la lumière des textes et de données en cours et de plusieurs exemples significatifs. Des procédures de sécurité informatique, incluant le respect des réglementations pour la protection des données personnelles, dont le RGPD, sont établies pour se protéger des violations de données : montrant par là même que sans sécurité, il n'existe pas de vie privée.

Dans ce contexte, le RGPD est fondé sur le droit fondamental universel à la vie privée (i.e., la protection contre toute immixtion arbitraire dans sa vie privée) établi par les Nations Unies après la Seconde Guerre mondiale, et dans un contexte de développement des moyens de communication. Le RGPD repose d'autre part sur le droit des citoyens de garder le contrôle de leurs données (notamment de décider des conditions de partage de ces informations).

Le RGPD est une référence internationale et de nombreuses réglementations sont mises en œuvre. Pourtant, le RGPD semble ne pas ralentir l'augmentation des violations de données (favorisées par le volume exponentiel de transferts de données). Et, nous constatons une forte variabilité entre pays européens dans les moyens d'action du RGPD (e.g., sanctions financières ou nombre de plaintes notifiées aux autorités nationales).

Ainsi pour éclairer notre question de recherche, portant sur l'influence de la culture sur le comportement de réponse face à une violation de données personnelles, il est nécessaire d'explorer l'état des recherches (i) tant sur les violations de données personnelles que (ii) sur l'influence de la culture sur le souci de contrôle de ses données personnelles.

Section 2. Contexte académique de la recherche

Pour éclairer notre question de recherche, portant sur l'influence de la culture sur le comportement de réponse face à une violation de données personnelles, notre objectif dans cette deuxième section est d'exposer l'état des recherches académiques portant (i) d'une part sur les violations de données personnelles et (ii) d'autre part sur l'influence de la culture sur le souci des individus de contrôler leurs données personnelles.

1. Causes et effets des violations de données personnelles

Les violations de données personnelles ont été traitées essentiellement en systèmes d'information (SI) et en sécurité informatique. Elles sont abordées de façon récente en sciences de gestion et font l'objet de peu de définitions (1.1.). Les recherches portent essentiellement sur les causes et conséquences techniques (1.2.) des violations de données personnelles. Et, les sciences de gestion se sont surtout intéressées aux conséquences financières pour les entreprises (1.3.). Ceci nous amène à faire état des recherches concernant les conséquences des violations pour les individus et les réponses apportées face à une violation de données personnelles (1.4.).

1.1. Définitions académiques des violations de données personnelles

Romanosky et al. (2013, p.125) définissent une violation de données « *au sens large comme la divulgation non autorisée d'informations personnelles par une organisation* ». Cette définition inclut tout type d'usage abusif de données personnelles, comme l'usage de cookies tiers par la publicité digitale et programmatique (que nous avons expliqué précédemment et que nous avons exclu). Par ailleurs, d'autres recherches définissent une violation de données comme un événement signalant la malversation d'un accès non autorisé aux données personnelles de parties prenantes (Culnan & Williams, 2009; Rasoulion et al., 2017).

Dans notre recherche, une violation de données personnelles est : tout vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif.

1.2. Causes et conséquences des violations de données personnelles

1.2.1. Causes techniques des violations de données personnelles

Dans ce paragraphe, nous reprenons et précisons certaines explications descriptives des violations de données personnelles, vues précédemment en introduction : ces explications nous ont permis d'établir la définition adoptée des violations de données personnelles.

Les causes à l'origine d'une violation de données personnelles peuvent être diverses : e.g., divulgation accidentelle, attaque de pirates informatiques, suppression inappropriée, attaque d'inités, source de données égarée ou vol d'équipement (Rasoulia et al., 2021). Les violations de données personnelles sont distinguées selon l'intention (violation intentionnelle ou non) et le mode d'accès aux données (cf. Tableau 4). Les auteurs ou les fraudeurs à l'origine de la violation peuvent avoir accès aux données de façon physique (perte d'un ordinateur pour le fauteur ou vol d'un ordinateur pour le fraudeur) ou de façon logique (e.g., contrôles d'autorisation d'accès à un serveur défectueux).

Les violations de données personnelles sont essentiellement intentionnelles et plus de 30% d'entre elles correspondent à des attaques d'inités, i.e., des violations intentionnelles des données par une personne ayant un accès légitime, comme un employé ou un contractant (Rasoulia et al., 2021). Les autres causes de violations de données sont dans 20% le vol d'équipements (i.e., la confiscation illégale d'équipements, tels que des ordinateurs portables, des smartphones, des dispositifs de mémoire portables, par des voleurs à l'intérieur ou à l'extérieur de l'entreprise), dans 18% l'attaque de pirates informatiques⁶², et dans 16% des cas la divulgation accidentelle (e.g., l'envoi de données à la mauvaise personne par courriel, télécopie ou courrier, en raison d'une erreur humaine accidentelle ou d'une erreur technique d'un équipement) (Rasoulia et al., 2021).

⁶² Les techniques les plus courantes de piratage informatique sont : (i) les ransomwares (i.e., une demande immédiate de rançon pour récupérer des données personnelles et des logiciels après prise de contrôle à distance d'un système), (ii) les malwares (i.e., une atteinte aux fichiers ou aux systèmes informatiques par l'injection d'un logiciel quelconque), (iii) le phishing (i.e., la récupération de données confidentielles par l'envoi d'un courriel exploitable), (iv) les attaques DDoS (Distributed Denial of Service), qui visent à saturer les requêtes d'un site, pour demande de rançon et chantage « au déni de service »).

Tableau 4 : Classification des violations de données selon leurs causes et points d'accès (Khan et al., 2021)

Catégorie	Définition	Exemples
Intentionnelles	Une violation causée par un acte malveillant dont l'intention est de nuire à une organisation	Pirates informatiques Accès non autorisés Initiés malveillants Acteurs parrainés par l'État Terroristes
Non intentionnelles	Une violation causée par des actions accidentelles, soit par un individu, soit par un processus, sans intention malveillante ⁶³	Comportement non sécurisé d'utilisateur Perte ou réutilisation des supports Logiciel défectueux Divulcation non autorisée Logiciel non autorisé
Physiques	Un point physique d'accès indésirable aux données sensibles	Dossier papier perdu Matériel informatique volé Dispositifs malveillants installés Accès physique non autorisé Ordinateur personnel non autorisé
Logiques	Un point logique d'accès indésirable aux données sensibles	Logiciel malveillant Infrastructure de réseau vulnérable Accès logique non autorisé Propriété intellectuelle volée Contrôles d'autorisation défectueux Logiciel défectueux

Exemple personnel :

Les modalités (intentionnelles ou non / physiques ou logiques) peuvent peut-être avoir un impact sur la perception de la violation de données. En effet, l'exemple présenté en Annexe 1 montre qu'un salarié de Visiativ avait téléchargé sans autorisation un fichier informatique contenant mes nom, prénom et numéro de sécurité sociale. Il s'agit alors clairement d'un vol d'informations personnelles intentionnel. Ma colère aurait été moins importante si cela avait été un incident non intentionnel et une erreur professionnelle pour laquelle Mercer et son prestataire Visiativ s'excusaient. Cet exemple personnel illustre le fait qu'une violation de données personnelles intègre des critères autres si elle est décrite par un utilisateur.

⁶³ E.g., 92 millions d'enregistrements ont été dévoilés accidentellement chez American On Line en 2005.

1.2.2. *Conséquences techniques des violations de données personnelles*

En sécurité informatique, l'impact d'une violation de données est évalué selon (i) le type de données affectées par la violation (e.g., données financières, numéro de sécurité sociale, informations médicales, informations générales ; Rasoulia et al., 2021), et (ii) le dommage porté sur les données (cf. Tableau 5 ; Khan et al., 2021).

Une violation de données peut endommager soit la confidentialité des données (l'objectif est de faire connaître ces informations à des tiers), soit leur disponibilité (l'objectif est de rendre ces données non accessibles et ainsi de bloquer certaines activités), soit leur intégrité (l'objectif est de supprimer ou de modifier certaines informations pour perturber certaines activités).

Tableau 5 : Impact des violations sur les données personnelles (Khan et al., 2021)

Catégorie	Définition	Exemples
Confidentialité	L'effet néfaste qu'auront les données consultées en dehors d'un besoin professionnel	Vol d'identité Amendes Poursuites judiciaires Perte d'un avantage concurrentiel Perte d'emploi
Disponibilité	Toute perte d'accès aux données ou aux ressources, quelle qu'en soit la durée	Déni de service Données volées Panne d'électricité Défaillance du système Données effacées
Intégrité	Toute manipulation non autorisée ou accidentelle de données stockées, en transit ou en cours d'utilisation, quelles que soient les parties concernées	Données modifiées Perte d'un avantage concurrentiel Données supprimées

Ces impacts techniques ont des conséquences financières pour les entreprises que nous précisons dans le paragraphe suivant.

1.3. Conséquences financières pour les entreprises

Les entreprises évaluent les conséquences des violations de données essentiellement en termes d'impact financier. En se basant sur la littérature à propos de la gestion des risques (Billings et al., 1980; Burnett, 1998), cet impact financier est analysé en deux étapes : (i) valeur de la perte des données violées (e.g. quelle est la valeur estimée des données volées ou endommagées ? Quelle est la perte financière générée par un non-accès momentané aux données ?) ; (ii) gravité du processus causal à l'origine de la brèche (e.g., pression temporelle pour résoudre le processus défectueux, degré de contrôle de l'entreprise sur le processus) (Rasoulion et al., 2021). Les violations de données personnelles ont un impact financier pour les entreprises à travers les frais de remise en service (disponibilité et intégrité des données), les pénalités éventuelles, et la possible baisse de valeur de l'entreprise liée à une perte de confiance du marché⁶⁴.

Ainsi, les recherches ont jusque-là essentiellement porté sur les coûts des litiges pour les entreprises (e.g., Romanosky et al., 2013), sur le cours des actions des entreprises (Acquisti et al., 2006 ; Cavusoglu et al., 2004 ; Foerderer & Schuetz, 2022 ; Malhotra & Kubowicz Malhotra, 2011 ; Martin et al., 2017), sur les risques réputationnels ou opérationnels des entreprises (e.g., Martin et al., 2017). Nous y voyons que les impacts sur les rendements boursiers sont proportionnellement aussi importants que le niveau de gravité de la violation de données (e.g., violation de données financières, attaques de pirates) (Rasoulion et al., 2021), que les grandes entreprises subissent une perte de valeur marchande plus importante que les petites entreprises, et que l'effet est surtout marqué sur le long terme (Malhotra & Kubowicz Malhotra, 2011). De plus, une violation de données personnelles par une entreprise génère une perte de confiance de ses clients et plusieurs recherches se sont intéressées à l'impact de la perte de confiance sur le cours boursier (Rasoulion et al., 2021; Confente et al., 2019).

Les entreprises vont, de ce fait, chercher à réduire le coût de la violation de données, notamment en réduisant les compensations apportées aux personnes dont les données ont été violées.

⁶⁴ En octobre 2020, Sopra Steria, leader dans la transformation numérique et l'édition de logiciels, avec 46.000 collaborateurs dans 25 pays, a subi un ransomware majeur : le personnel n'a pas pu accéder à ses e-mails et fichiers pendant plusieurs jours et une rançon de 2 millions d'euros a été payée. Les coûts estimés de l'attaque pour l'entreprise un mois plus tard s'élèveraient à 50 millions d'euros (Sopra Steria expects €50 million loss after Ryuk ransomware attack, 25.11.2020, disponible à : <https://www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/>)

Finalement, les coûts pour les entreprises intègrent également ceux des actions mises en place pour diminuer le risque qu'une nouvelle violation de données se produise (e.g., actions de prévention pour réduire le risque, par de la sensibilisation, de la formation, de l'évaluation de risques), des actions pour limiter la portée des violations (e.g., système de détection des incidents), et des actions pour réduire les impacts financiers (e.g., assurance cybersécurité) (Confente et al., 2019 ; Chan & Palmeira, 2021 ; Rasoulilian et al., 2021).

1.4. Conséquences des violations pour les individus et réponses apportées

1.4.1. Préjudices des violations pour les individus et citoyens

Face à une violation de leurs données personnelles, les individus reçoivent généralement de faibles compensations (Solove & Hartzog, 2022). De façon générale, « *la littérature qui traite des manquements à la vie privée des entreprises omet largement les implications pour les consommateurs dans le cadre conceptuel du problème* » (Martin & Murphy, 2017, p.148). Romanosky et al. (2013) ont exploré le processus des poursuites pour violation de données, depuis la plainte jusqu'au règlement. Ils indiquent que seulement 3,7 % d'un échantillon de violations de données américaines signalées entre 2000 et 2010 ont fait l'objet d'un procès devant un tribunal fédéral. La probabilité d'un procès augmente proportionnellement au nombre de données perdues et à leur sensibilité (e.g., données bancaires), à la présence d'un préjudice réel démontrable, et au type de violations (e.g., piratage informatique, perte de matériel).

Cependant, les conséquences des violations personnelles peuvent s'avérer dramatiques, poussant certaines personnes au suicide, comme nous l'avons vu précédemment. Pour permettre une bonne interprétation juridique des préjudices liés à une violation de données personnelles, évitant ainsi que celles-ci ne donnent lieu à aucune réparation faute de préjudice identifiable, Citron & Solove (2021) ont proposé une typologie des préjudices (cf. Tableau 6).

Tableau 6 : Typologie de préjudices de violations de données personnelles (Citron & Solove, 2021)

	Explications
Préjudices physiques	Entraînent des blessures corporelles ou la mort (e.g., meurtre d'une actrice dont l'adresse a été retrouvée sur Internet ; suicide d'une personne comme dans le scandale Ashley Madison cité ci-avant)
Préjudices économiques	Impliquent des pertes monétaires ou de quelque valeur de quelque chose. Dans ce cas, certaines violations sont faciles à démontrer (e.g., vol de carte bancaire ou d'identité numérique)
Préjudices de réputation	Les atteintes à la réputation et au statut d'un individu dans la communauté (e.g., diffamation)
Préjudices psychologiques	Toute une série de sentiments négatifs et variés tels que l'anxiété, l'angoisse, la préoccupation, etc., qui peuvent être classés en deux grandes catégories : la détresse émotionnelle (i.e., implique des sentiments douloureux ou désagréables) et la perturbation (i.e., implique une atteinte à la tranquillité et à la paix de l'esprit)
Préjudices d'autonomie	Consistent à restreindre, inhiber ou influencer les choix des personnes (générant des effets de coercition, manipulation, défaut d'information)
Préjudices de discrimination	Désavantagent les personnes en raison de leur sexe, de leur race, de leur origine nationale, de leur orientation sexuelle, de leur âge, de leur appartenance à un groupe ou d'autres caractéristiques ou affiliations
Préjudice relationnel	Impliquent la détérioration de relations importantes pour la santé, le bien-être, les activités de la vie et le fonctionnement de la société

Le type de préjudices aura très probablement une influence sur le comportement de réponses des individus face à une violation de leurs données personnelles. Quelques recherches explorent les effets psychologiques provoqués par une violation, que nous précisons dans le paragraphe suivant.

1.4.2. Conséquences psychologiques des violations des données personnelles

Quelques études révèlent les perceptions et conséquences psychologiques que les violations de données peuvent avoir. Une violation de données est avant tout perçue comme une rupture de contrat entre l'entreprise et ses clients. Les clients évaluent l'importance de cette rupture contractuelle selon certaines caractéristiques de propriété, de degré d'intimité ou de valeur des données (Krafft et al., 2021). Ces sentiments négatifs à l'égard de l'entreprise envers laquelle le consommateur faisait implicitement confiance pour sécuriser les données collectées ont un impact sur les réponses apportées par le consommateur (Labrecque, 2021). Pour cela, Malhotra & Kubowicz Malhotra (2011) montrent que les entreprises devraient considérer les violations de données personnelles non pas comme des défaillances de leurs systèmes d'information mais plutôt comme des défaillances de leurs services client.

Par ailleurs, le stress et les émotions négatives causées par la violation de données impactent les réponses apportées par le consommateur (Labrecque, 2021). La violation de données génère évidemment une perte de confiance (Bansal & Zahedi, 2015) qui influence le comportement de réponse, ce comportement pouvant varier selon le degré (fort ou faible) de préoccupation pour la protection de ses données personnelles (Bansal et al., 2015). Enfin, les violations de données personnelles sont un signal de vulnérabilité adressé aux clients (Martin, 2018), que les dispositions des entreprises en matière de transparence et de contrôle compensent.

En synthèse, quatre effets psychologiques d'une violation de données personnelles sont identifiés : le sentiment de rupture de contrat, le stress, la perte de confiance, la vulnérabilité perçue.

1.2.3. Réponses des individus face aux violations de données personnelles

Quelques recherches explorent les comportements de réponses apportées face à une violation de données personnelles :

- En reprenant la littérature sur le comportement de plainte du consommateur, Son & Kim (2008) établissent une taxonomie des réponses pour la protection de la vie privée (divulgations d'informations, actions privées ou publiques) ;
- Mills & Harclerode (2018) identifient deux catégories d'actions personnelles : (i) mettre en place des moyens de se protéger contre d'éventuelles futures violations de données et (ii) décider de continuer les poursuites judiciaires. Dans ce deuxième cas, des barrières semblent exister (e.g. le 1^{er} amendement aux États-Unis qui s'oppose à la protection des données personnelles⁶⁵) et les poursuites judiciaires sont complexes ;
- Janakiraman et al. (2018) étudient l'effet d'une annonce de violation de données personnelles sur le comportement d'un client d'une chaîne de distribution multi-enseignes. Alors que la violation de données ne concerne qu'une seule enseigne du groupe de distribution, Janakiraman et al. (2018) prouvent qu'un client, dont les données ont été violées, va continuer de fréquenter les enseignes du groupe, tout en diminuant de manière significative ses dépenses et en migrant d'une enseigne à l'autre au sein de la chaîne de distribution ;
- Selon Labrecque (2021), les réponses face à une violation sont adressées à l'entreprise (e.g., falsification d'informations) ou visent à protéger le consommateur (e.g., changement de mot de passe, notification publique de la violation).

Malgré cela, les réponses des consommateurs à une violation de leurs données personnelles ont encore été très peu étudiées (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018). Notre recherche vise à combler cette lacune.

⁶⁵ La liberté d'expression garantie par le 1^{er} amendement de la Constitution aux USA est en contradiction avec la protection de données personnelles : la liberté d'expression justifie l'usage à tout type de données (e.g., annulation en 2011 d'une loi du Vermont interdisant aux laboratoires pharmaceutiques d'exploiter les données des ordonnances pour dresser le profil des médecins prescripteurs, cette loi limitant la liberté d'expression des entreprises. Confer Les Echos (03.08.2018) : Protection des données : l'Amérique peut-elle suivre l'Europe ? (accessible à <https://www.lesechos.fr/2018/04/protection-des-donnees-lamerique-peut-elle-suivre-leurope-987980>)

*

Nous venons de préciser les causes des violations de données personnelles (essentiellement intentionnelles) et leurs conséquences techniques sur les données (e.g., disponibilité, intégrité). Nous avons montré que les entreprises évaluent les conséquences des violations essentiellement sur des critères financiers (valeurs des données affectées, coûts de remise en service, baisse des cours boursiers). Nous avons précisé les préjudices pour les individus (e.g., physiques, réputationnels, discriminatoires), et notamment psychologiques (e.g., stress, perte de confiance, vulnérabilité ressentie), ayant un impact sur les réponses apportées (e.g., mise en place de protection, changement de fournisseur). Or, les recherches sur ces comportements de réponse face à une violation de données personnelles manquent peut-être du fait qu'elles sont essentiellement conduites en systèmes d'information (SI) et en sciences juridiques.

En synthèse, le Tableau 7 reprend les éléments identifiés et moins connus par la recherche à ce jour :

Tableau 7 : État des recherches portant sur les violations de données personnelles

Ce qui est bien connu	Ce qui est moins connu
- Définir une violation de données personnelles selon des critères techniques (causes, conséquences) et de sécurité informatique	- Définir une violation de données personnelles telle que perçue et comprise par des individus, citoyens, usagers ou clients
- Intégrer l'impact des violations de données personnelles sur la confiance des clients dans un objectif d'évaluation du risque financier pour les entreprises	- Comprendre les comportements individuels en matière de sécurité informatique pour réduire le risque - Comprendre les implications pour les consommateurs afin de les dédommager et/ou de les protéger
- Classifier les préjudices des violations de données personnelles	- Identifier les conséquences psychologiques des violations - Comprendre le lien préjudice, conséquences et réponses aux violations

Nous allons dans la partie suivante exposer le deuxième volet de notre contexte académique : l'état des recherches portant sur l'influence de la culture sur le souci de contrôle de ses données personnelles.

2. Culture et souci de contrôle des données personnelles

Dans ce paragraphe, notre objectif est de comprendre comment la recherche a jusqu'alors abordé la question de l'influence de la culture sur le souci de contrôle de ses données personnelles (méthodes, pays, référentiels culturels) et quels principaux résultats sont apparus. Pour cela : nous définissons le souci de contrôle des données personnelles (2.1.), nous identifions l'ensemble des recherches portant sur l'influence de la culture sur le souci de contrôle des données personnelles (2.2.), nous classons ces recherches selon les méthodes, modèles et dimensions culturelles utilisés (2.3.) avant d'analyser les résultats obtenus (2.4.).

2.1. Définition du souci de contrôle des données personnelles

Comme précédemment exposé, le RGPD repose sur le droit des citoyens de contrôler l'accès à leurs données personnelles, ce qui nous amène à nous interroger sur l'état des recherches portant sur l'influence de la culture sur le souci de contrôle de ses données.

Les recherches ont jusqu'alors porté sur l'influence de la culture sur l'*information privacy concern*, i.e., « le souhait des individus, groupes ou institutions de déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées aux autres » (Westin, 1967, p.7), ou bien encore « la capacité de gérer des informations sur soi-même » (Belanger et al., 2002, p.249) : en somme, le souci d'un individu de contrôler l'utilisation potentielle par des tiers de ses données personnelles. Nous reprendrons plus en détail dans le chapitre 2 l'historique de la conceptualisation de l'*information privacy concern*.

Ces recherches ont donc cherché le lien entre la culture et le souci de contrôle de ses données personnelles : en quoi une caractéristique ou dimension culturelle va-t-elle plus ou moins faire varier ce souci de contrôle de ses données personnelles ? Nous les détaillons ci-après.

Nota bene : dans les tableaux suivants (Tableaux 6, 7, 9, 10 et 11), par souci de synthèse, « PC » est l'acronyme de *Privacy Concern*, i.e., le souci de contrôle de ses données personnelles .

2.2. Recherches interculturelles sur la protection des données personnelles

2.2.1. *Identification des recherches interculturelles portant sur la protection de la vie privée*

À l'aide de revues de littérature récentes (i.e., Beke et al., 2018; Li et al., 2022; Miltgen & Peyrat-Guillard, 2014), que nous avons complétées par des recherches par mots clés sur Google Scholar, nous avons identifié **28 recherches** qui portent sur l'influence de la culture sur le souci de contrôle de ses données (cf. Annexe 2).

Ces recherches ont été conduites entre 1977 et 2022, avec une accélération depuis 10 ans (12 recherches menées depuis 2012). Il ne s'agit pas d'une revue de littérature systématique.

Alternativement, ces recherches :

- étudient l'influence directe de la culture sur le souci de contrôle de ses données,
- explorent l'influence de la culture sur un comportement qui fait intervenir le souci de contrôle de ses données (e.g., utilisation des réseaux sociaux),
- font des comparaisons internationales du souci de contrôle de ses données (sans forcément étudier l'impact direct de la culture), ou d'un comportement qui fait intervenir le souci de contrôle de ses données.

De ce fait, nous avons fait le choix d'exclure certaines recherches (intéressantes) car elles n'étudient pas l'influence de variables culturelles, ou ne font pas de comparaisons entre pays (e.g., recherche d'Alkis & Kose (2022) qui étudie en Europe les préoccupations relatives à la protection de la vie privée dans les activités de commerce électronique ; recherche de Grosso et al. (2020) qui étudie l'effet de la confiance sur le souhait de partage d'informations personnelles, avec une approche multi-niveaux macro, méso et micro dans 14 pays).

Pour chaque recherche, nous exposons les informations principales de manière synthétique (méthode, pays, dimensions, etc.) et ne précisons pas si la culture est étudiée comme une variable indépendante ou une variable modératrice : ce point est discuté à la fin de notre thèse (chapitre 7).

2.2.2. *Classification des recherches interculturelles portant sur la protection de la vie privée*

Ces 28 recherches comprennent :

- 1 recherche séminale conduite par Altman en 1977 (cf. paragraphe § 2.2.3) ;
- 6 recherches comparant des comportements entre pays sans modèle (§ 2.2.4) ;
- 1 recherche mobilisant un modèle culturel autre que celui d'Hofstede (§ 2.2.5) ;
- 20 recherches qui mobilisent le modèle culturel d'Hofstede (§ 2.3).

Toutes ces recherches témoignent de l'effet de la culture sur le souci de contrôle de ses données.

Près des trois quarts de ces recherches (20 sur 28) utilisent le modèle d'Hofstede (Hofstede, 1984, 2001; Hofstede et al., 2010) et parmi elles, toutes mobilisent la dimension d'individualisme (i.e., une préférence pour la défense de ses buts et intérêts personnels). La très grande majorité des recherches défendent l'idée que l'individualisme accroît le souci de contrôle de ses données personnelles (e.g., Krasnova & Veltri, 2010; Liu & Wang, 2018; Miltgen & Peyrat-Guillard, 2014). Cependant, certaines recherches identifient un effet de la culture sans isoler un effet spécifique de l'individualisme (Milberg et al., 1995) et deux recherches pointent un effet négatif (Bellman et al., 2004; Lowry et al., 2011) : le consensus n'est donc pas total.

En parallèle, il est intéressant de mettre en perspective ces recherches « mainstream » avec les huit autres recherches plus spécifiques (§ 2.2.3, 2.2.4 et 2.2.5). Parmi elles, la recherche d'Altman (1977) est essentielle à notre thèse. Ce dernier conseille d'analyser les effets de la culture sur la vie privée de manière globale, et de récentes recherches reviennent au même constat d'approche globale tout en citant Altman (1977) (e.g., Li et al., 2022). Les autres recherches interculturelles sur la vie privée, qui ne mobilisent aucun modèle, sont intéressantes, car, selon nous, elles laissent la place à une large compréhension des phénomènes : par exemple, en différenciant les niveaux de compréhension de la vie privée entre souci de protection de ses données personnelles et le souci de protection de sa vie privée dans ses interactions sur les réseaux sociaux (e.g., Gurău & Ranchhod, 2009; Li et al., 2022).

2.2.3. *Recherche séminale d'Altman (1977)*

La recherche d'Altman (1977), qui repose sur un de ces anciens travaux (Altman, 1975), offre l'une des premières définitions de la vie privée et met l'accent sur la capacité de l'individu à exercer une certaine forme de contrôle. Altman reprend l'idée que le concept de vie privée est composé de dimensions d'autonomie personnelle, d'identité et d'estime de soi (Westin, 1967). La vie privée est, en ce sens, un contrôle d'un accès sélectif à son *moi*. Ces recherches (Altman, 1975, 1977) ne portent pas spécifiquement sur le contrôle de ses données ou informations personnelles.

Altman (1977) défend l'idée que « *la vie privée est un processus universel qui implique des mécanismes de régulation propres à chaque culture* » (Altman, 1977, p.66). Ceci signifie qu'il n'existe pas de sociétés pour lesquelles la vie privée est importante et d'autres pour lesquelles la vie privée ne l'est pas. De plus, chaque culture va développer des mécanismes qui lui sont propres pour définir « *les limites et les frontières du moi / soi* » (p.68), i.e., les dimensions d'autonomie personnelle, d'identité et d'estime de soi. Ces mécanismes d'adaptation des dimensions de la vie privée portent sur le langage, l'espace, les relations sociales, avec des propriétés très diverses. Ces mécanismes d'adaptation interviennent à différents niveaux propres à chaque culture. Si le contrôle de son intimité s'exerce à un certain niveau dans une culture (e.g., fermer la porte de chez soi) et que ce phénomène ne se retrouve pas dans une autre culture, il ne faut pas en conclure que cette culture n'exerce pas de contrôle de son intimité. Au contraire, il faut rechercher, avec d'autres niveaux d'observation, comment cette culture exerce un contrôle de sa vie privée, car elle le fait : la vie privée est un phénomène universel.

Altman (1977) soutient que « *pour examiner la vie privée en tant que phénomène interculturel, le niveau d'analyse doit être déplacé des comportements particuliers de vie privée vers une analyse plus holistique, semblable à un modèle* » (Altman, 1977, p.70). Nous en retenons la nécessité de suivre une démarche à plusieurs niveaux d'observation pour étudier l'influence de la culture sur le comportement de réponse face à une violation de données personnelles.

2.2.4. *Recherches comparant des pays*

Toutes les recherches ci-dessous comparent des pays sans intégrer de dimensions culturelles. Elles sont regroupées dans le Tableau 8.

Les recherches interculturelles sur la vie privée ne mobilisant aucun modèle portent un intérêt du fait qu'elles laissent la place à une large compréhension des phénomènes. D'ailleurs, Pentina (2016) se refuse à utiliser un modèle précis ou à chercher des différences (cette recherche met en lumière le fait que les jeunes Chinois et les jeunes Américains ne se différencient pas sur le souci de partage de leurs données personnelles).

Maynard & Taylor (1996) démontrent, quant à eux, que les Japonais et les Américains ont une attitude comparable vis-à-vis du marketing direct, mais qu'étonnamment, les Japonais ont un souci plus important du contrôle de leurs données personnelles. Ils expliquent ce résultat surprenant en le rapprochant de la coutume japonaise du « uchi-soto » (i.e., une gestion particulière de la vie privée entre sphère privée et sphère publique).

Plus tard, Gurău & Ranchhod (2009) comme Li et al. (2022) différencient les niveaux de souci de vie privée entre souci de contrôle de ses données personnelles, souci de contrôle de ses interactions personnelles, ou souci de contrôle de la confidentialité de ses échanges personnels. Les auteurs révèlent qu'en Roumanie, en Chine et en Corée, le souci de contrôle de ses données personnelles est moins élevé qu'au Royaume-Uni, en France ou aux États-Unis ; en revanche, la préoccupation pour la façon dont la vie privée peut être contrôlée par l'extérieur ou les institutions (e.g., liberté d'expression, liberté de rencontres) est supérieure.

En effet, selon Gurău & Ranchhod (2009), le pays d'origine influence la perception des risques liés au souci de protection de ses données personnelles : ceci est confirmé par Cecere et al. (2015). Les auteurs attestent qu'au sein d'un même espace européen et, malgré un cadre institutionnel relativement homogène, le cadre institutionnel national influence le souci de contrôle de ses données personnelles. Cependant cette étude a été réalisée avant l'entrée en vigueur du RGPD, suite à quoi la notoriété du RGPD a fortement augmenté dans toute l'Europe (certaines études Eurobarometer nous en apportent la preuve⁶⁶) : les résultats de cette étude doivent donc être pris en considération avec vigilance.

⁶⁶ Special Eurobarometer 487a - 2019 (https://data.europa.eu/data/datasets/s2222_91_2_487_eng?locale=en)

Tableau 8 : Recherches interculturelles sur la vie privée comparant des pays

Référence	Attitudes et comportements étudiés	Méthodes et pays	Résultats concernant PC
Maynard et Taylor (1996)	Attitude générale par rapport au marketing direct (MD) et à la divulgation de données personnelles	États-Unis vs Japon Enquête (questionnaire)	Préoccupation pour la protection de la vie privée plus élevée au Japon (culture collectiviste)
Gurău & Ranchhod (2009)	Confidentialité dans le commerce mobile	Royaume-Uni, France et Roumanie Enquête (questionnaire)	Le pays d'origine influence 1) la perception des risques afférents à la PC, 2) les stratégies de protection. En Roumanie : sentiment d'intrusion des messages non sollicités moins important ; mais niveau de risque perçu des messages élevé et niveau de confiance institutionnelle pour protéger la vie privée faible.
Hann et al. (2007)	e-commerce	États-Unis vs Singapour Expérimentation	Pour les consommateurs américains, l'utilisation secondaire non autorisée est un problème mineur ≠ pour les consommateurs singapouriens, il s'agit de la violation de la vie privée la plus importante lorsqu'ils traitent avec des détaillants en ligne.
Cecere, Le Guel, Soulié (2015)	Préoccupations des individus en matière de vie privée liées aux risques sur les réseaux sociaux	23.087 individus dans 28 pays européens	Le cadre institutionnel garantissant des efforts nationaux pour protéger la vie privée augmente la probabilité de s'inquiéter d'une éventuelle utilisation abusive des données privées.
Pentina (2016)	Téléchargement et adoption d'applications mobiles faisant appel à des informations sensibles	États-Unis vs Chine	Bien que les cultures américaine et chinoise diffèrent sur différentes dimensions reconnues académiquement (e.g., auto-direction, indépendance, sécurité), cette recherche ne formule aucune hypothèse. Elle montre que la culture n'a aucune influence sur le partage d'informations de la part des Millénials américains et chinois.
Li et al. (2022)	Décisions des internautes en matière de gestion de la vie privée sur les réseaux sociaux (RS)	États-Unis, Corée, Chine	Les utilisateurs de RS aux États-Unis sont plus préoccupés par la confidentialité des informations, tandis que les utilisateurs coréens et chinois sont plus préoccupés par la confidentialité interactionnelle (contrôle et maîtrise des rencontres faites en ligne) et par la confidentialité psychologique (liberté d'expression des opinions).

2.2.5. *Recherches utilisant d'autres modèles que celui d'Hofstede*

Nous avons identifié une seule recherche utilisant un modèle autre que celui d'Hofstede (cf. Tableau 9). Selon Zakaria et al. (2003), l'adoption de nouvelles technologies de communication est différente selon les niveaux de contextualisation acceptés (Hall, 1976). Dans les cultures à contexte élevé, la communication est implicite et s'appuie fortement sur le contexte, en valorisant les relations interpersonnelles alors que les cultures à faible contexte s'appuient sur une communication verbale explicite. Les auteurs montrent, en particulier pour les pays du Moyen-Orient, l'importance de la confiance (qui se gagne par des interactions physiques en face à face), et le rôle très relatif du souci de protection de la vie privée dans les échanges, qui est plus spécifique aux cultures à faible contexte (Ting-Toomey & Kurogi, 1998).

Cependant, nous aurions aussi pu ajouter dans cette partie la recherche de Dinev et al. (2006) qui mobilise à la fois le modèle d'Hofstede et la théorie de la confiance de Fukuyama (1995) (cf. Tableau 13) : en effet, les auteurs considèrent que le modèle d'Hofstede ne suffit pas à expliquer les différences de confiance entre les États-Unis et l'Italie, la confiance étant un facteur influençant fortement le souci de contrôle de ses données personnelles.

Tableau 9 : Recherches en *cross-cultural privacy* utilisant d'autres modèles qu'Hofstede

Référence	Comportements étudiés	Méthodes et pays	Dimensions culturelles	Résultats concernant PC
Zakaria et al. (2003)	Réactions des individus aux applications informatiques liées à la communication	Pays du Middle East	Communication à contexte faible ou élevé (Hall, 1976)	Importance de concevoir des technologies de communication qui facilitent l'interaction en face à face et la communication orale à distance (messagerie audio, vidéoconférence)

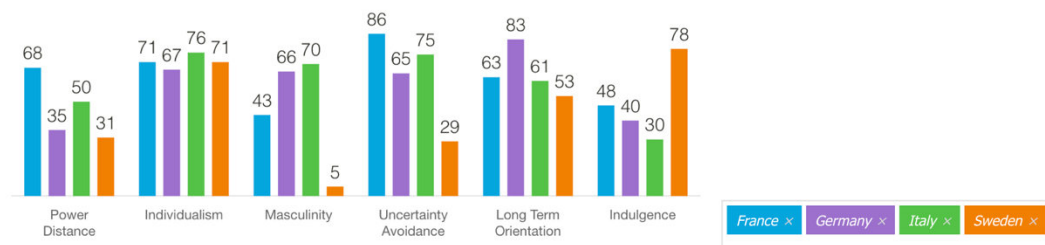
2.3. Recherches mobilisant le modèle de la culture nationale d'Hofstede

2.3.1. Présentation du modèle de la culture nationale d'Hofstede

Le modèle d'Hofstede (1980, 2001, 2010) provient d'un vaste projet de recherches conduit auprès de salariés de filiales d'IBM dans plus de 50 pays. Les recherches d'Hofstede sont basées sur la compréhension des cultures nationales, dépendant par exemple de la langue, de la religion ou de l'histoire commune. Plus précisément, Hofstede considère la distance culturelle, c'est-à-dire l'aspect d'une culture qui peut être mesuré par comparaison avec d'autres cultures (Hofstede et al., 2010), définie sous forme de dimensions.

Pour Hofstede (1980), la culture est une programmation mentale collective. Hofstede définit 6 dimensions : distance hiérarchique, individualisme, masculinité, contrôle de l'incertitude, orientation à long terme et indulgence⁶⁷ (cf. définitions dans le Tableau 10 et exemples de valeurs dans la Figure 6).

Figure 6 : Exemples de valeurs de dimensions d'Hofstede pour quelques européens⁶⁸



⁶⁷ En anglais et sur la figure, respectivement : power distance, individualism, masculinity, uncertainty avoidance, long-term orientation et indulgence

⁶⁸ <https://www.hofstede-insights.com/>

Tableau 10 : Définitions des 6 dimensions d'Hofstede

Dimensions d'Hofstede		Explications
Hofstede (1984) a d'abord identifié 5 dimensions de la culture nationale sur la base de 116.000 questionnaires collectés entre 1967 et 1973 auprès de plus de 60.000 répondants	Distance hiérarchique	Le degré selon lequel les membres les moins puissants d'une société acceptent et s'attendent à ce que le pouvoir soit distribué de manière inégale.
	Individualisme	Une préférence pour un cadre social dans lequel les individus sont censés ne s'occuper que d'eux-mêmes et de leur famille proche.
	Masculinité	Une préférence pour une société valorisant l'accomplissement, l'héroïsme et l'affirmation de soi (par opposition à la coopération, la modestie, le souci des plus faibles et la qualité de vie).
	Contrôle de l'incertitude	Le degré selon lequel les membres d'une société se sentent mal à l'aise face à l'incertitude et à l'ambiguïté.
Hofstede a ensuite ajouté 2 dimensions à son modèle initial (Hofstede, 2001 ; Hofstede et al., 2010).	Orientation à long terme	Le degré selon lequel les comportements sont guidés par un certain pragmatisme et des résultats à long terme, considérant la relation « passé-présent-futur », et ne se limitant pas à des traditions séculaires et des normes strictes pour préparer l'avenir. Bien que « peu de recherches empiriques aient intégré cette cinquième dimension » (Moalla, 2016, p.33), la version à 5 dimensions du modèle de Hofstede semble plus pertinente et conforme aux prédictions des modèles de Schwartz et de GLOBE (Girerd-Potin et al., 2018).
	Indulgence	Une préférence pour la satisfaction des besoins par rapport à des normes sociales strictes pour réguler la société. Cette dernière dimension a été beaucoup moins étudiée que les précédentes, ce qui en rend sa compréhension et son interprétation moins aisées.

2.3.2. Recherches concentrées sur la dimension d'individualisme

Dans le Tableau 11, nous indiquons pour chacune des dimensions d'Hofstede le nombre de recherches qui la mobilisent sur le total de 20 recherches identifiées. Nous prenons en considération chacune des dimensions considérées au début de chaque recherche, même si celle-ci est exclue ensuite dans l'analyse, notamment pour des problèmes de multicollinéarité. Par exemple, Cho et al. (2009) excluent au cours de leur analyse deux dimensions (distance hiérarchique et masculinité) mais nous les intégrons dans le tableau 8 ci-dessous.

Nous constatons que toutes les recherches mobilisent l'individualisme, considéré comme une dimension clé dans le comportement de protection de vie privée (Miltgen & Peyrat-Guillard, 2014). Les recherches établissent alors un lien entre une préférence culturelle pour des intérêts individuels et le souci de défense de ses droits individuels et de contrôle de ses données personnelles.

Dans une moindre mesure, le contrôle de l'incertitude, la distance hiérarchique et la masculinité sont mobilisés. Nous adoptons les abréviations suivantes dans les tableaux qui suivent : PC pour souci de protection de la vie privée (*Privacy Concern*), PD pour distance hiérarchique (*Power Distance*), IND pour individualisme, UA pour contrôle de l'incertitude (*Uncertainty Avoidance*), MAS pour masculinité, LTO pour orientation à long terme (*Long Term Orientation*) et IDL pour indulgence.

Tableau 11 : Nombre d'occurrences des dimensions d'Hofstede dans les recherches mobilisant le modèle

Hofstede dimensions	Distance hiérarchique (PD)	Individualisme (IND)	Contrôle de l'incertitude (UA)	Masculinité (MAS)	Orientation à long terme (LTO)	Indulgence (IDL)
Nombre de recherches utilisant cette dimension sur 20 recherches	6	20	11	5	1	1

De ce fait, nous utilisons l'individualisme pour répartir en 3 groupes les 20 recherches identifiées :

- Celles qui ne montrent aucune influence de l'individualisme sur le souci de contrôle de ses données personnelles (Tableau 12 = 2 recherches),
- Celles qui montrent une influence positive (Tableau 13 = 16 recherches),
- Celles qui montrent une influence négative (Tableau 14 = 2 recherches).

Les Tableau 12, Tableau 13, Tableau 14 sont présentés ci-après et sont suivis d'analyses (§ 2.3.3).

Tableau 12 : Recherches mobilisant le modèle d'Hofstede sans identifier d'effets spécifiques des dimensions culturelles

Référence	Comportements étudiés	Méthodes et pays	Dimensions d'Hofstede	Résultats concernant la PC
Milberg et al. (1995)	Concern for Information Privacy and regulation	30 pays Enquête (N=900)	PD, IND, UA	Pas d'effet de PD, IND et UA sur la PC
Li et al. (2017)	Prédiction des décisions des personnes en matière de protection de leur vie privée	8 pays (E.g., Canada, Chine, Allemagne, US, Suède, Inde) Méthode d'apprentissage automatisé	PD, IND, UA, MAS, LTO, IDL	IND et IDL ont un pouvoir prédictif plus important que les autres dimensions

Tout d'abord, si Milberg et al. (1995) n'identifie étonnamment pas d'effet particulier d'une dimension sur le souci de contrôle de ses données personnelles, les auteurs soulignent eux-mêmes les limites de leur recherche (e.g., échantillon, valeurs culturelles limitées et agrégées) : une nouvelle recherche est ensuite effectuée et montre l'influence positive de trois dimensions (distance hiérarchique, individualisme, masculinité) (Milberg et al., 2000).

De plus, nous devons préciser que la recherche de Li et al. (2017) a pour objectif d'évaluer le pouvoir prédictif des dimensions culturelles d'Hofstede sur les décisions à venir en matière de protection de la vie privée. Dans ce cadre, cette recherche atteste que l'individualisme (ainsi que l'indulgence) a un pouvoir prédictif plus important, et met ce constat au regard du fait que l'individualisme est une dimension importante, favorisant généralement un souci plus important pour la protection de ses données personnelles.

Tableau 13 : Recherches mobilisant le modèle d'Hofstede montrant un souci de protection de la vie privée plus important dans les pays individualistes

Référence	Comportements étudiés	Méthodes et pays	Dimensions d'Hofstede	Résultats concernant PC
Milberg et al. (2000)	Attitude à l'égard des approches réglementaires et de la gestion des entreprises	19 pays (e.g., Italie, Inde, Japon, États-Unis, Australie, Finlande, Allemagne, France) Enquête (N=595)	PD, IND, UA, MAS	Effet positif de PD, IND et MAS sur PC Effet négatif de UA sur PC
Dinev et al. (2006)	Décision d'achat en ligne	États-Unis et Italie Enquête en ligne (N=1.300)	UA et IND + Fukuyama's trust theory	Effet positif de IND sur PC Effet négatif de UA sur PC
Steenkamp & Geyskens, (2006)	Valeur perçue lors de visites sur des sites Internet	23 pays sur 3 continents 30 sites Internet (N=8.886)	IND	Effet positif de IND sur PC
Muk (2007)	Adoption de SMS publicitaires	US vs Taiwan (N=376)	IND	Effet positif de IND sur PC (mais IND et COLL considèrent différents aspects)
Cho et al. (2009)	Préoccupation pour la protection de ses données en ligne	Bangalore, Séoul, Singapour, Sydney, NY (N=1.261)	PD, IND, UA et MAS	Effet positif de IND sur PC Effet négatif de UA sur PC
Krasnova & Veltri (2010)	Divulgaration de soi sur les réseaux sociaux	Allemagne et États-Unis (N=491)	IND	Effet positif de IND sur PC
Posey et al. (2010)	L'auto-divulgaration des communautés professionnelles en ligne	Royaume-Uni et France Enquête en ligne (N=529)	IND	Effet négatif de IND sur la divulgation de soi en ligne → effet positif de IND sur PC
Tsoi & Chen (2011)	Problèmes de confidentialité liés à l'utilisation de réseaux sociaux	France vs Hong Kong	IND, UA	Effet positif de IND sur PC
Krasnova et al. (2012)	Dévoilement, création et partage de contenu sur les réseaux sociaux	Allemagne et USA	IND, UA	IND et UA modèrent l'impact de la PC et de la confiance perçue sur la divulgation de soi en ligne
Chen et al., (2013)	M-commerce	États-Unis et Corée (N=540)	IND	Effet positif de IND sur PC
Miltgen & Peyrat-Guillard (2014)	Divulgaration ou protection des données à caractère personnel	7 pays européens Focus groups (N=14)	IND	Effet négatif de IND sur la divulgation de soi en ligne → effet positif de IND sur PC

Park et al. (2015)	Utilisation des réseaux sociaux	États-Unis et Corée du Sud (N=977)	IND	IND modère la relation entre la PC et le degré d'utilisation des réseaux sociaux
Yang & Kang (2015)	Importance du partage d'informations pour la planification de campagnes publicitaires	Taiwan et États-Unis (N=113)	IND	Effet positif de IND sur PC
James et al. (2017)	Partage d'informations sur les réseaux sociaux	États-Unis et Corée du Sud	IND	Effet positif de IND sur PC
Trepte et al. (2017)	Perceptions des risques liés à la vie privée et des gratifications sur les réseaux sociaux (RS))	5 pays (Allemagne, Pays-Bas, Royaume-Uni, États-Unis, Chine) (N=1.550)	IND et UA	Effet négatif de IND sur les gratifications sociales Effet positif de UA sur la perception des risques et bénéfices sur les RS
Liu & Wang, (2018)	Gestion des limites de la vie privée sur les sites de réseaux sociaux	États-Unis et Chine (N=831)	IND et UA	Les normes de groupe ont un effet plus fort sur les récompenses sociales et le contrôle de la vie privée sous un collectivisme élevé

Tableau 14 : Recherches mobilisant le modèle d'Hofstede montrant un souci de protection de la vie privée moins important dans les pays individualistes

Référence	Comportements étudiés	Méthodes et pays	Dimensions d'Hofstede	Résultats concernant PC
Bellman et al. (2004)	Attitudes générales envers le PC et la réglementation	38 pays (e.g. Argentine, Malaisie, Japon, États-Unis, Royaume-Uni) Enquête	PD, IND, UA et MAS	Effet négatif de PD, IND et MAS sur PC
Lowry et al., (2011)	Instant messaging (IM)	États-Unis vs China Enquête en ligne	UA, PD, IND et MAS	Forte influence : 1) des dimensions culturelles sur PC, 2) de PC sur l'intention d'utiliser et l'usage direct de l'IM

2.4. Conclusion des recherches interculturelles sur le souci de contrôle de ses données personnelles

2.4.1. Résultats observés

Les recherches prouvent l'influence de la culture sur le souci de contrôle de ses données personnelles. Or si cette question est explorée dans plusieurs situations (e.g., e-commerce, réseaux sociaux, applications mobiles), il semble manquer une compréhension claire et approfondie des mécanismes d'influence de la culture et des mécanismes sociologiques ou psychologiques reliant la culture aux intentions ou comportements.

Par ailleurs, les recherches mobilisent essentiellement le modèle d'Hofstede et sa dimension d'individualisme, partant du principe qu'une préférence pour la défense de ses propres intérêts et objectifs est une dimension clé dans le souci de contrôle de ses données personnelles. Ces recherches offrent un premier éclairage précieux à notre sujet. Elles mettent majoritairement en lumière le fait que les individus issus de pays « individualistes » ont une préoccupation plus grande pour la protection de leur vie privée et le contrôle de leurs données personnelles (e.g., Milberg et al., 2000).

Cependant, des résultats contradictoires apparaissent. Milberg et al. (2000) comme Bellmann et al. (2004) soulignent une influence significative de l'individualisme, de la distance au pouvoir et de la masculinité, mais dans des directions strictement opposées. Lowry et al. (2011) observent que les étudiants chinois sont plus concernés par la protection des données personnelles que les étudiants américains plus individualistes, contredisant ainsi les recherches marquant une plus forte préoccupation pour la vie privée dans les pays individualistes (e.g., Dinev et al., 2006; Miltgen & Peyrat-Guillard, 2014; Posey et al., 2010). De même, Miltgen & Peyrat-Guillard (2014) soulignent que « *certaines recherches indiquent que les personnes issues de cultures nationales fortement individualistes ont moins de préoccupation pour la protection de leur vie privée et sont plus à l'aise avec des niveaux élevés de divulgation de données (TingToomey, 1991)* » (Miltgen & Peyrat-Guillard, 2014, p.107). Enfin, les recherches indiquent également que les consommateurs venant de différents pays ont des préoccupations différentes (e.g., Gurău & Ranchhod, 2009). Par exemple, les consommateurs américains attribuent beaucoup d'importance à l'utilisation secondaire non autorisée de données personnelles par des vendeurs en ligne, contrairement aux consommateurs singapouriens (Hann et al., 2007). Ce constat invite à plus explorer d'autres modèles et dimensions de la culture.

En synthèse, le Tableau 15 reprend les éléments identifiés et moins connus par la recherche à ce jour :

Tableau 15 : État des recherches portant sur l'influence de la culture sur le souci de contrôle de ses données personnelles

Ce qui est bien connu	Ce qui est moins connu
- Constater l'influence de la culture sur le souci de contrôle de ses données personnelles	- Expliquer les mécanismes d'influence (e.g., variable médiatrice ou modératrice, autres effets) - Explorer les mécanismes reliant culture et comportements
- Explorer la dimension d'individualisme d'Hofstede	- Explorer les autres modèles culturels et les autres dimensions du modèle d'Hofstede
- Constater qu'une préférence pour l'individualisme amène un plus grand souci de contrôle de ses données personnelles	- Constater le phénomène inverse : c'est-à-dire qu'une préférence pour le collectivisme amène à un moindre souci de contrôle de ses données personnelles

En conséquence, il persiste un appel sans équivoque et unanime à de plus amples recherches.

2.4.2. *Appels à de plus amples recherches*

Plusieurs chercheurs appellent à de plus amples recherches :

- « *La variation nationale et interculturelle des préférences et des croyances en matière de protection de la vie privée représente un domaine de recherche nécessaire pour l'avenir* » (Martin & Murphy, 2017, p.140) ;
- « *Il est nécessaire de mieux comprendre l'influence de la culture sur les préoccupations en matière de protection de la vie privée* » (Beke et al., 2018, p.44) ;
- « *Des questions subsistent (...) concernant les différences culturelles et la manière dont elles influencent les attentes des consommateurs en matière de protection réglementaire de la vie privée. Les consommateurs de diverses cultures apprécient-ils une protection forte ou préfèrent-ils la liberté de choix et l'autodétermination en matière de confidentialité des données ?* » (Martin et al., 2020, p.11) ;
- « *Les recherches qui intègrent les valeurs culturelles dans un cadre incluant les préoccupations en matière de vie privée et de réglementation restent rares* » (Benamati et al., 2021, p.131) ;
- « *Les différences culturelles sont (...) susceptibles d'influencer la perception des consommateurs à l'égard des expériences sociales avec l'IA (...) des recherches futures devraient explorer leurs conséquences interpersonnelles et sociétales plus larges* » (Puntoni et al., 2021, p.15).

Synthèse de la section sur le contexte académique

Dans cette section, nous montrons que les violations de données personnelles sont essentiellement intentionnelles et que les entreprises les évaluent surtout en termes d'impacts financiers. Nous précisons les préjudices pour les individus (e.g., physiques, réputationnels, discriminatoires), et notamment psychologiques (e.g., stress, perte de confiance, vulnérabilité ressentie), ayant un impact sur les réponses apportées (e.g., mise en place de protection, changement de fournisseur). Cependant, les recherches sur ces comportements de réponse face à une violation de données personnelles sont peu nombreuses.

D'autre part, nous montrons que les recherches interculturelles portant sur le souci de contrôle de ses données personnelles ont très majoritairement mobilisé le modèle de la culture nationale d'Hofstede et sa dimension d'individualisme. Si ces recherches présentent un souci de contrôle de ses données personnelles plus important pour les individus valorisant l'individualisme, des résultats contradictoires interrogent et appellent à de plus amples recherches. Nous précisons également la recherche d'Altman (1977) qui préconise une approche globale et à plusieurs niveaux pour toute recherche portant sur la vie privée, ainsi que des recherches comparant des pays et permettant de spécifier différents niveaux de perception de la vie privée (e.g., faible souci de contrôle de ses données personnelles mais fort souci de contrôle de ses interactions sur les réseaux sociaux).

Par conséquent, une plus ample exploration de la littérature sur différents champs est nécessaire afin d'éclairer notre question de recherche portant sur l'influence de la culture sur le comportement de réponses face à une violation de ses données personnelles. Nous précisons pour cela dans la section suivante nos axes de recherches et les contributions attendues.

Section 3. Axes de recherche et contributions attendues

Comme nous venons de le voir, le nombre de violations de données personnelles est en très forte augmentation, en parallèle de la mise en place de réglementations internationales, adoptées de façon variable par les citoyens et les consommateurs. Face à cette situation, les réponses des consommateurs à une violation de leurs données personnelles ont été peu étudiées (Mamonov & Benbunan-Fich, 2018). La recherche s'est intéressée au souci de contrôle de ses données personnelles, et à l'influence de la culture sur celui-ci. Si les recherches ont montré que la culture a un effet indiscutable sur le souci de contrôle des données personnelles (Miltgen & Peyrat-Guillard, 2014), elles appellent à de nouvelles explorations.

Ainsi, notre recherche adresse la question suivante : Quelle est l'influence de la culture sur le comportement de réponses face à une violation de ses données personnelles ?

Précisément, notre recherche vise à répondre à trois questions :

1. Quelles sont les réponses face à une violation de données personnelles ?
2. Quelle est l'influence de la culture sur ces réponses ?
3. Quels mécanismes psychologiques et sociologiques relient la culture aux réponses ?

Quelles sont les réponses face à une violation de ses données personnelles ?

Les réponses possibles face à une violation de ses données personnelles peuvent être très variables, depuis le souhait de ne rien faire, d'en parler haut et fort, jusqu'à la volonté de porter plainte. Pour cela, les comportements de réponses face à une violation de données personnelles doivent être rapprochés des comportements de protection de la vie privée (*information privacy protective responses*), pour être mieux compris, ce que nous ferons dans la revue de littérature.

Cependant, il est nécessaire de différencier les réponses de protection de la vie privée, qui s'expriment a priori et font appel à une conscience de la protection de la vie privée, des réponses face à une violation de données constatée, qui s'expriment a posteriori. Partant du principe qu'une violation de données personnelles correspond à une rupture du contrat qui lie un consommateur à une organisation (Labrecque, 2021), une exploration du champ du comportement de plainte des consommateurs (*consumer complaint behaviour - CCB*) pourra nous éclairer sur les mécanismes de réponses face à une insatisfaction constatée. Cela nous

aidera à comprendre si les réponses des consommateurs face à une violation de leurs données correspondent aux réponses de plaintes classiques des consommateurs insatisfaits, et sinon, comment elles s'en différencient.

Enfin, toute la difficulté dans la compréhension des comportements de réponse face à une violation de données personnelles réside dans la variabilité des niveaux de gravité perçue. Le comportement de réponse peut-il être observé de la même manière qu'il s'agisse d'informations intimes (e.g., fréquentations sexuelles) ou d'informations moins stratégiques (e.g., liste de courses alimentaires) ? Cette question doit être mise au regard d'un fait divers assez connu : en 2012, un père de famille accuse le responsable d'un magasin Target à Minneapolis d'encourager les grossesses d'adolescentes après que sa fille a reçu de la part du magasin des bons de réduction pour des articles de maternité. Quelques jours plus tard, il apprend que celle-ci était enceinte : les achats de la jeune fille retracés par sa carte de fidélité Target, et analysés par un programme prédictif de Target, avaient permis d'identifier la grossesse de l'adolescente⁶⁹. Ceci nous permet d'insister sur le fait qu'il n'existe pas d'informations personnelles plus ou moins sensibles que d'autres. En revanche, beaucoup de personnes pensent « ne rien avoir à cacher » : leurs comportements de réponse face à une violation de données peuvent-ils s'en trouver affectés ?

Quelle est l'influence de la culture sur ce comportement de réponse ?

Les recherches interculturelles portant sur le souci de contrôle de ses données personnelles ont été essentiellement conduites en systèmes d'information (SI) avec une approche positiviste et en mobilisant le modèle d'Hofstede qui est le modèle le plus utilisé en SI (Miltgen & Peyrat-Guillard, 2014 ; Dinev et al., 2006). Jusqu'en 2010, la majorité de la littérature s'appuie sur l'étude d'un seul pays, les États-Unis (Bélanger & Crossler, 2011), à l'exception de quelques grandes études internationales (Bellman et al., 2004 ; Milberg et al., 1995, 2000 ; Steenkamp, 2001). Quelques études ont adopté une perspective transnationale mais évaluent les différences entre les États-Unis et un autre pays, nécessitant de faire varier les pays explorés (Li, 2011; Pavlou, 2011; Smith et al., 2011).

⁶⁹ New York Times (2012) : How Companies Learn Your Secrets (accessible à : <https://www.nytimes.com/2012/02/19/magazine/shopping-habits>)

Ces différentes recherches sont précieuses et l'usage principal du modèle d'Hofstede apporte un premier éclairage essentiel à la compréhension des phénomènes culturels spécifiques au souci de protection de sa vie privée. À partir de cela, nous identifions 4 voies d'exploration pour enrichir la compréhension des phénomènes. Il s'agirait de :

- Aller au-delà des approches essentiellement hypothético-déductives,
- Mobiliser des modèles autres que celui de la culture nationale d'Hofstede,
- Déplacer la focale au-delà de la notion d'individualisme,
- Adopter une approche autre que celle macro et environnementale de la culture.

En effet, la culture est considérée uniquement comme une variable environnementale et macro (Beke et al., 2018), au même niveau que la législation. La recommandation de démarche globale d'Altman (1977) ne semble pas prise en considération. Les dimensions culturelles sont considérées indépendamment : il serait donc intéressant de mieux comprendre comment les relations entre les dimensions culturelles et les construits représentant la préoccupation pour la protection de la vie privée s'opèrent à différents niveaux selon des contextes culturels différents (Liu & Wang, 2018).

Une récente étude permet d'illustrer cette nécessité d'approche multi-niveaux. Martin & Palmatier (2020) montrent à travers une très large étude cross-culturelle que si les réglementations en matière de protection de la vie privée (e.g., RGPD, CPRA) s'imposent aux distributeurs en ligne internationaux, ceux-ci doivent non seulement intégrer de manière proactive et rapide ces problématiques de protection de la vie privée dans leurs échanges avec leurs clients-consommateurs, mais également développer des approches internationales cohérentes en matière de *privacy*, indépendamment des réglementations en vigueur. Pour cela, il est nécessaire de comprendre comment les réglementations mettent le consommateur à l'aise, comment se déroule la relation entre individu et gouvernement et ainsi quel est le juste équilibre entre mécanismes du marché (de l'entreprise) et mécanisme régulateur (gouvernemental). De ce fait, une approche plus holistique intégrant des niveaux macro (institutionnel et régulateur), méso (organisations) et micro (psychologie du consommateur) est requise.

Nous avons, en effet, besoin de mieux comprendre les fondements théoriques du concept de culture pour que notre recherche mobilise des angles conceptuels de la culture différents, dans l'espoir d'apporter une vision différente de l'influence de la culture.

Quels mécanismes psychologiques et sociologiques relient la culture aux réponses ?

Les recherches sur l'adoption de nouvelles technologies connectées ou sur le comportement de divulgation de données personnelles ont beaucoup porté sur la compréhension de la place de l'*information privacy concern*, défini comme le souci de protection de sa vie privée et de contrôle de ses données personnelles (Belanger et al., 2002; Westin, 1967). Or, nous nous interrogeons sur le rôle central du souci de contrôle de ses données personnelles dans les mécanismes psychologiques de réponses face à une violation de données personnelles. À notre sens, un éclairage des effets culturels offrira une nouvelle perspective à la compréhension de ce concept. Nous suivons l'appel de Dinev (2014, p.99) formulé dans un éditorial du *European Journal of Information Systems* : « *Comprendre les origines anthropologiques et culturelles de la vie privée aidera également à comprendre les différentes approches réglementaires et les besoins des nations en matière de vie privée.* »

En effet, le souci de protection de la vie privée est un concept abstrait (Bandara et al., 2018). Le lien entre besoin de vie privée et préoccupation pour la protection des données personnelles peut ne pas être évident et rester abstrait pour des raisons éducatives, économiques, ou culturelles. Par exemple, Pasquier (2018) indique qu'il existe un usage très collectif des supports informatiques (smartphones ou ordinateurs) au sein des familles modestes, pour des raisons économiques mais aussi par résistance à l'individualisation que génèrent ces usages ; ainsi qu'une très grande distance avec la question de la protection des données à caractère personnel. De plus, le droit à la vie privée a été défini comme droit universel à la suite de la Seconde Guerre mondiale pour éviter tout usage de listages d'individus ayant mené aux rafles de personnes juives : les bases historiques de la définition du droit à la vie privée en font un concept intrinsèquement culturel. Il en résulte de façon évidente une influence de certains traits et normes culturelles sur la préoccupation pour la vie privée, spécifiques à certains pays ou groupes sociaux. À la lumière des effets culturels, le souci de contrôle de ses données personnelles peut apparaître sous de nouveaux aspects et son rôle aussi. Nous avons au préalable besoin de mieux en comprendre la conceptualisation et les fondements théoriques, ce que nous allons faire dans la partie suivante.

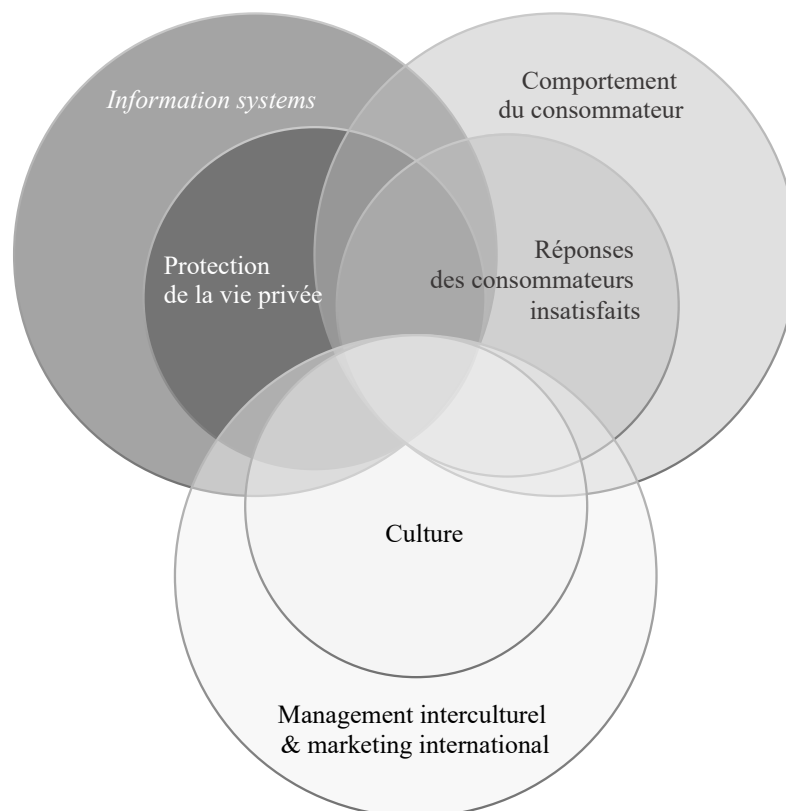
Par ailleurs, face à une violation de données personnelles, d'autres antécédents comme la sécurité ou l'atteinte à l'intégrité peuvent être plus concrets et influencer plus fortement les réponses. Soit d'autres mécanismes psychologiques doivent être identifiés, soit le souci de contrôle de ses données personnelles doit évoluer en conceptualisation pour couvrir tous les

aspects nécessaires pour être généralisable internationalement : « *la question de savoir si les utilisateurs de différents pays se concentrent sur différents types de préoccupation pour la protection de la vie privée reste ouverte* » (Li et al., 2022, p.2).

Enfin, le comportement de réponse face à une violation de données personnelles peut faire également appel d'autres mécanismes sociétaux importants comme la capacité à agir et la pression sociale à agir : il est alors nécessaire d'en expliquer les fondements et de les explorer.

Pour répondre à ces questions, la partie suivante présentera les fondements théoriques de notre recherche autour de trois axes : la préoccupation pour la protection de la vie privée, issue essentiellement du champ des systèmes d'information ; les réponses des consommateurs insatisfaits, issus du champ du comportement du consommateur et du *consumer complaint behaviour* ; la culture, issue du champ du management interculturel et du marketing international ; comme représenté sur la Figure 7 ci-après.

Figure 7 : Champs académiques des fondements théoriques de la thèse



Synthèse de la section sur les axes de recherche et contributions attendues

Notre recherche explore la question de l'influence de la culture sur le comportement réponses face à une violation de ses données personnelles. Et plus précisément, elle vise (i) à identifier les réponses face à une violation de données personnelles, comportement encore peu étudié, ce qui nécessite d'explorer la littérature sur le comportement de plainte du consommateur, tout en tenant compte des spécificités du contexte des violations de données (e.g., la conscience des risques). Notre recherche a ensuite pour objectif (ii) d'identifier l'influence de la culture sur le comportement de plainte, en tenant compte de 4 limites identifiées dans les recherches précédentes (i.e., une approche essentiellement hypothético-déductive, un modèle essentiellement de la culture nationale d'Hofstede, un focus sur la notion d'individualisme et une approche macro et environnementale de la culture). Enfin notre recherche souhaite (iii) identifier les mécanismes psychologiques et sociologiques qui relient la culture aux réponses.

Pour cela, nous avons besoin de mieux comprendre les fondements théoriques (i) de la protection des données personnelles (ii) des comportements de réponses en cas d'insatisfaction (iii) de la culture, pour que notre recherche mobilise des angles conceptuels différents, dans l'intention d'apporter une vision nouvelle. Le chapitre suivant est consacré à ces fondements théoriques.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

**Protection
des données
personnelles**

**Réponses des
consommateurs
insatisfaits**

**Culture
et valeurs**



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :
Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :
Influence des
normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :
Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 2. Fondements théoriques



Ce deuxième chapitre portant sur les fondements théoriques de notre recherche a pour objectif d'explorer trois champs de la littérature (la protection de la vie privée, le comportement de plainte et la culture) afin d'identifier des angles conceptuels différents nous amenant à éclairer notre question de recherche : quelle est l'influence de la culture sur le comportement de réponse face à une violation de données personnelles ?

La première section est consacrée au souci de contrôle des données personnelles. Notre objectif vise à comprendre les fondements académiques de la protection de la vie privée, les grandes définitions et conceptualisations de la préoccupation pour la protection des données personnelles, et les théories mobilisées pour expliquer les arbitrages économiques, sociétaux et psychologiques en matière de protection de la vie privée.

Dans la deuxième section, nous nous intéressons aux réponses des consommateurs insatisfaits et au comportement de plainte des consommateurs, dans le but de mieux apprécier les comportements de réponses pour la protection des données personnelles, encore peu étudiés. Une troisième section portera sur la culture, dont nous présentons les fondements historiques et les grandes acceptations, avant de nous concentrer sur les valeurs culturelles (définitions et modèles conceptuels).

Section 1. Protection des données personnelles

“Privacy isn’t just about personal data”, Solove, D.J., 04.05.2022, Tweeter

1. Conceptualisation de la protection de la vie privée

Cette partie vise à mieux comprendre les conceptualisations de la protection de la vie privée et des données personnelles. Pour cela, nous faisons un rappel historique de l’émergence de la protection de la vie privée dans les différents champs académiques (1.1), nous détaillons les définitions, conceptualisations et possibles traductions apportées à la protection de la vie privée (1.2), ainsi que les dimensions de contrôle, transparence et confiance (1.3). Enfin, nous montrons que la compréhension et la conceptualisation de la protection de la vie privée peuvent être dépendantes du contexte dans lequel ce souci de protection s’exerce (1.4).

1.1. Émergence de la protection de la vie privée dans le champ académique

La *privacy concern* est une préoccupation pour la protection de la vie privée de l’individu, née à la fin du XIX^{ème} siècle avec l’émergence des médias. Nous avons vu dans le chapitre introductif comment le concept de vie privée a été intégré comme droit humain universel fondamental, sur lequel sont fondées nos réglementations en la matière. Dans ce paragraphe, la vie privée a été abordée avec des perspectives différentes selon les disciplines.

Le respect de la vie privée est un sujet ancien, traité par exemple en philosophie, en psychologie ou en sociologie. La vie privée comporte trois dimensions : le secret (i.e., le choix de partager quand on veut les informations nous concernant), la quiétude ou la possibilité d’isolement social (i.e., ne pas être ennuyé par les sollicitudes et les intrusions) et l’autonomie individuelle (i.e., le désir humain d’indépendance par rapport au contrôle des autres) (Rochelandet, 2010). Altman (1975) souligne que le concept de vie privée est composé de dimensions d’autonomie personnelle, d’identité et d’estime de soi (Westin, 1967). La vie privée est alors un contrôle

d'un accès sélectif à son *moi*. Enfin la notion de vie privée prend des formes différentes à travers les époques et les cultures (Ariès & Duby, 1985).

Dans un contexte de développement des moyens de communication, plusieurs disciplines, comme l'économie, les sciences juridiques, les sciences sociales, la psychologie, les systèmes d'information, se sont intéressés à la définition de la vie privée (Stone et al., 1983), en se concentrant sur l'*information privacy*, ou vie privée informationnelle, qui porte plus particulièrement sur les informations que nous partageons (communications et données personnelles). La vie privée est en effet un concept polymorphe avec 4 dimensions (Burgoon et al., 1989) :

- La vie privée physique, i.e., la protection de son espace personnel et l'évitement de toute intrusion physique qui affecte au moins un des sens,
- La vie privée interactionnelle, i.e., la protection et la gestion des relations et des interactions sociales,
- La vie privée psychologique, i.e., la protection de sa réflexion et de son état psychologique, cognitif et émotionnel,
- La vie privée informationnelle, à laquelle notre recherche s'intéresse, i.e., « le contrôle sur la manière dont les informations personnelles sont acquises et utilisées » (Pavlou, 2011, p.977).

Dans les années 70, plusieurs économistes de l'école de Chicago discutent du bien-fondé économique de la protection légale de la vie privée ; ils considèrent les données personnelles comme des ressources immatérielles. Défenseurs de la libre exploitation des données personnelles, ils considèrent que les droits fondamentaux constitutionnels garantissent la liberté individuelle, l'inviolabilité du domicile, la protection contre la diffamation. Il n'est alors pas nécessaire d'ajouter un droit supplémentaire qui protège les données personnelles, et la rétention d'informations personnelles peut s'avérer dangereuse car elle limite la transparence et les possibilités de contrôle pour la sécurité de chacun (Posner, 1978). Ils s'opposent aux défenseurs du respect à tout prix de la vie privée. Ces derniers, héritiers de la philosophie des Lumières, considèrent que la vie privée est le socle de toute liberté individuelle et une condition essentielle à la liberté d'action permettant à chacun de se développer, à l'abri du contrôle des autres : sans vie privée individuelle, pas de société libre. Les théories de l'école de Chicago ont été beaucoup critiquées : e.g., position conservatrice tournée vers les intérêts des industriels et confondant *corporate privacy* et *personal privacy* ; vision unidimensionnelle de la vie privée,

réduite à la dimension de secret (Hirshleifer, 1980), absence de prise en compte des externalités (Rochelandet, 2010). Mais elles trouvent un écho lorsque la vie privée se heurte à des impératifs publics. Par exemple, Etzioni (2004) soutient que réduire les possibilités individuelles de contrôle de sa vie privée atténuerait les besoins de contrôle et d'intrusion étatique, idée à la base de l'USA Patriot Act mis en place après le 11.09.01.

Par ailleurs, la protection de la vie privée et des données personnelles se trouve à l'intersection de plusieurs champs : économie, comme nous venons de le voir (les données personnelles étant une ressource immatérielle), sciences juridiques (laissant parfois un flou, comme par exemple l'article 9 du Code civil français qui stipule la nécessité de protéger la vie privée sans en définir ni le contenu ni les contours ; Rochelandet, 2010), et systèmes d'information (qui se focalisent sur la sécurité informatique sans prise en compte des comportements individuels ; Solove & Hartzog, 2022). Le marketing s'intéresse, quant à lui, assez tardivement à la vie privée (à partir des années 2000) : le marketing étudie comment « *la collecte, le stockage, l'utilisation d'informations, la transparence et le contrôle (par le consommateur)* » (Beke et al., 2018, p.6) peuvent influencer les attitudes, les perceptions et le comportement du consommateur.

Notre travail vise à prolonger ces recherches en marketing en étudiant la construction de l'équilibre entre vie privée et sécurité et entre contrôle de données personnelles et sécurité.

1.2. Définitions et conceptualisations de la protection des données personnelles

1.2.1. Définitions différentes selon les disciplines et les périodes

De ces différents travaux dans des disciplines variées découlent plusieurs définitions de la vie privée (cf. Tableau 16). D'abord définie comme *"the right to be let alone"* (Warren & Brandeis, 1890) dans une période de développement de la photographie, la vie privée informationnelle (Clarke, 1999; Smith et al., 2011) s'inscrit comme le désir individuel de pouvoir contrôler ou influencer l'acquisition et l'utilisation potentielle de ses données personnelles par des tiers (Belanger et al., 2002 ; Westin, 1967). Elle repose essentiellement sur le fait qu'un individu est maître de ses données. La préoccupation pour la protection de la vie privée s'est accrue avec la sophistication des moyens de communication et l'accessibilité des données personnelles, qu'il s'agisse d'informations sociodémographiques, de profils ou d'historiques de recherche déclarés volontairement ou enregistrés automatiquement (Georges, 2009 ; Cardon, 2019).

Tableau 16 : Différentes définitions de la vie privée (Martin & Murphy, 2017)

Définition	Source	Éléments complémentaires
État ou condition d'être libre d'être observé et dérangé ou pas, par d'autres personnes	Oxford English Dictionary	Définition commune de la vie privée en général.
Le droit d'être laissé tranquille (<i>The right to be left alone</i>)	Warren & Brandeis (1890)	Définition judiciaire célèbre, bien qu'il n'existe pas de droit constitutionnel US autonome.
État d'accès limité aux informations : « le souhait des individus, groupes ou institutions de déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées aux autres » (p.7)	Westin (1967)	L'état de la vie privée peut être défini comme un objectif qui mérite d'être atteint et préservé. Les déterminants de la vie privée sont l'anonymat, la solitude, la réserve et l'intimité.
Le contrôle d'un accès sélectif à son moi (<i>self</i>)	Altman (1975)	L'une des premières définitions de la vie privée à mettre l'accent sur la capacité de l'individu à exercer une certaine forme de contrôle.
« La capacité de gérer des informations sur soi-même » (p.249) (<i>right to control access to own personal information</i>)	Belanger (2002)	
Revendication de flux d'informations personnelles appropriés selon les contextes sociaux distincts	Nissenbaum (2010)	Préconise de définir des contraintes au flux d'informations selon le contexte, plutôt que de déterminer si l'information elle-même est privée ou publique.

1.2.2. Concept basé sur le contrôle et l'auto-gestion de ses données personnelles

Les sciences sociales, quant à elles, ont défini la vie privée en se basant sur la théorie de l'échange, et plus particulièrement sur la base de la théorie du contrat social qui « *stipule que les règles de partage des informations du consommateur doivent tenir compte de l'objectif de l'échange, du risque et des préjudices potentiels pour le consommateur* » (Martin & Murphy, 2017, p.144). Cette définition repose sur le principe selon lequel un individu peut gérer ses propres données, principe nommé *self-data management* (Solove, 2013). Du *self-data management* résultent les principes forts des réglementations actuellement en vigueur tels que le consentement, les droits de retrait ou d'effacement.

Cependant, si ces définitions ont été élaborées dans un contexte de demande relativement contrôlée de données personnelles (e.g., marketing direct), cela soulève des questions autour de l'explosion de la collecte de données, des cookies tiers, du big data et de l'utilisation de l'intelligence artificielle (e.g., Dignum, 2019). Les individus peuvent se sentir incapables de contrôler pleinement leurs données personnelles, du fait d'un effet « black box » de la collecte et du volume gigantesque des informations concernées. Pour prendre en compte ce phénomène, la vulnérabilité qui en découle (Del Bucchia et al., 2021) met également les comportements de résistance des personnes face à ce phénomène (Li et al., 2020), de nouvelles définitions et conceptualisations pourraient être envisagées. Il deviendrait donc pertinent d'intégrer des dimensions applicables à différents contextes culturels.

Le point commun à toutes les définitions de la vie privée est la notion de contrôle. Or le contexte actuel montre que cet exercice de contrôle est de plus en plus complexe. Notre recherche consiste donc à interroger la pérennité de la notion de « contrôle » dans la définition de la préoccupation pour la protection de ses données personnelles et de sa vie privée, à la lumière (i) d'une part des effets culturels, et (ii) d'une mise en contexte des violations de données personnelles.

1.2.3. *Conceptualisations différentes et changeantes*

Différents proxys ont été développés pour mesurer le degré de préoccupation pour la protection de ses données personnelles. Ils sont « *opérationnalisés comme un ensemble de croyances, attitudes et perceptions des consommateurs concernant leur vie privée* » et « *apparaissent comme un antécédent, conséquence et force modératrice dans un certain nombre de premières études sur la vie privée* » (Martin & Murphy, 2017, p.136) : cf. Tableau 17.

Ces proxys intègrent essentiellement les dimensions de contrôle et de transparence que nous allons expliquer dans la partie suivante (1.3). De plus, partant du constat que l'*information privacy concern* est un concept dépendant du contexte (ce que nous expliquons aussi dans la partie suivante 1.4), de nouvelles dimensions sont proposées au fur et à mesure : e.g., Zhang et al. (2022) proposent d'ajouter des dimensions pour prendre en compte les échanges de données personnelles entre pairs. Or compte tenu de l'explosion des usages et du volume de données personnelles (cf. supra), nous nous interrogeons fortement sur la pertinence d'ajouter de nouvelles dimensions au fur et à mesure des évolutions des contextes.

Tableau 17 : Conceptualisation et échelles en matière de protection de la vie privée

Auteurs	Conceptualisation	Dimensions
Smith et al. (1996)	Concern for Information Privacy (CFIP)	Collecte, utilisation secondaire non autorisée, accès inapproprié, erreurs
Malhotra et al. (2004)	Internet Users's Information Privacy Concern (IUIPC)	Collecte, contrôle, sensibilisation
Dinev & Hart (2004)	Perceived Privacy Concern	Capacité de contrôle perçue, vulnérabilité perçue
Hong & Thong (2013)	Internet Privacy Concern (IPC)	Gestion des interactions (collecte, utilisation secondaire, erreurs), gestion de l'information (accès inapproprié et contrôle), sensibilisation.
Li et al. (2020)	Privacy Concerns for Traceable Information (PCTI)	Temporal and Movement regularity
Zhang et al. (2022)	Peer Privacy Concern (PPC)	Information Privacy, Psychological Privacy, Communication Privacy, Virtual territory Privacy.

Face à ce constat, nous jugeons qu'il n'est pas pertinent de multiplier les nouvelles conceptualisations dépendantes essentiellement des contextes d'observation (cf. paragraphe 1.4 ci-après). Nous privilégions une conceptualisation plus générale, englobant un juste équilibre entre vie privée, personnalisation et sécurité (Dinev, 2014). Notre thèse s'appuie sur le premier aspect « vie privée – sécurité ». D'autres recherches portent sur les aspects de personnalisation (et de paradoxes de la vie privée que nous n'abordons pas ici).

1.2.4. Concept considéré de plus en plus comme abstrait

Comme nous le préciserons dans la partie suivante, le souci de contrôle de ses données personnelles joue un rôle central dans le comportement en ligne des consommateurs (Smith et al., 2011), comme les achats en ligne ou les contributions des communautés. Le comportement en ligne du consommateur est influencé par des facteurs, soit facilitateurs (i.e., le contrôle perçu de ses données, la transparence perçue des marques), soit inhibiteurs (i.e., les risques perçus ou les préoccupations concernant la confidentialité des informations) (Dinev et al., 2006). Ces facteurs sont notamment ancrés dans la confiance perçue dans la technologie ou les institutions (Lippert & Swierzcz, 2005 ; Mothersbaugh et al., 2012) et la responsabilité, qu'elle soit sociétale ou individuelle (Miltgen & Peyrat-Guillard, 2014). Les recherches sur la psychologie de la vie privée et la formation des préoccupations des consommateurs en matière de protection de la vie privée sont principalement basées sur le modèle APCO (Antecedent - Privacy Concern - Outcomes ; Smith et al., 2011 ; Dinev et al., 2015). Le modèle APCO donne au souci de contrôle de ses données personnelles (*information privacy concern*) une place centrale entre antécédents (individuels ou contextuels) et résultats (*outcomes* ; divulgation ou non des données).

Cependant, le principe d'autonomie et de responsabilisation des consommateurs vis-à-vis de leurs données personnelles, tout comme le rôle central de la préoccupation pour la protection de la vie privée, est remis en question. D'une part, il existe un paradoxe de la vie privée, i.e., un écart entre les préférences déclarées pour la protection de la vie privée mais distantes et abstraites (Bandara et al, 2018) et le comportement réel en termes de divulgation de la vie privée (Pavlou, 2011), qui privilégie des solutions en ligne plus concrètes. D'autre part, si le concept de la préoccupation pour la protection de la vie privée a été développé dans un contexte de sollicitation relativement contrôlée des données personnelles (e.g., marketing direct ou mailing

postal), il soulève des questions face à l'explosion des données, à l'utilisation du Big data et de l'intelligence artificielle (Dignum, 2019), aux techniques de publicité ciblée ou de suivi en ligne subreptice (Martin & Murphy, 2017), et à l'effet boîte noire de la collecte de données (e.g., vendeur en ligne invisible, suivi non déclaré ; Pasquale, 2015). Les techniques actuelles de collecte et d'usage des données personnelles rendent les consommateurs moins conscients de cette collecte de données, moins autonomes et plus vulnérables (Martin et al., 2017). La préoccupation pour la protection de la vie privée reste un concept abstrait (Bandara et al., 2018; Hallam & Zanella, 2017), et plusieurs recherches ont mobilisé la théorie de la distance psychologique pour éclairer les comportements paradoxaux lors des arbitrages liés à la vie privée. Nous les détaillons dans la partie suivante.

1.2.5. Traduction française d'information privacy concern

La recherche portant sur la protection de la vie privée est très majoritairement anglophone et utilise le terme d'*information privacy concern*. À notre connaissance, il n'existe pas à ce jour un travail conceptuel permettant d'apporter une traduction en français de ce terme.

En début de mémoire, et en nous basant sur la définition classique de *l'information privacy concern*, i.e., la capacité à contrôler l'usage et la partage de ses informations personnelles (Belanger et al., 2002), nous avons traduit *information privacy concern* par « **souci de contrôle de ses données personnelles** ». Nous avons fait le choix d'exclure tout de suite le terme « contrôle de sa vie privée », afin de nous concentrer sur la question de la protection des données personnelles.

De plus, les réglementations actuellement en cours continuent de se baser sur une maîtrise de ses données personnelles (e.g., notions de consentement éclairé, droit d'effacement ou de retrait). La notion de contrôle des données reste très présente, même si nous l'interrogeons face à une vulnérabilité informatique grandissante.

1.3. Dimensions de la préoccupation pour la protection de la vie privée

1.3.1. Contrôle et transparence

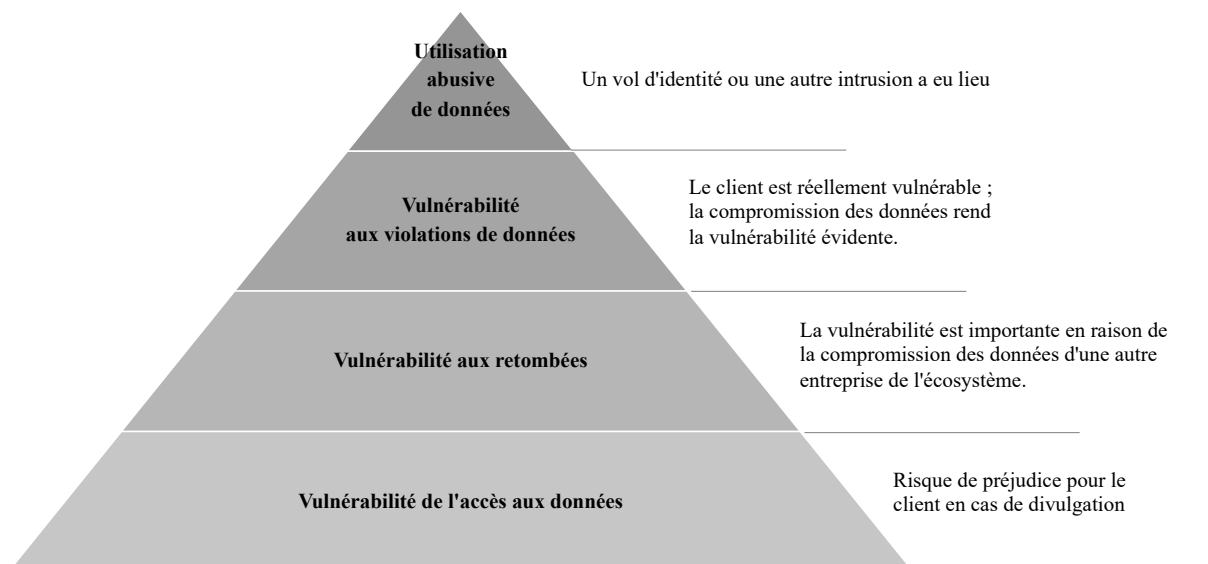
Parmi les dimensions clés définissant la préoccupation pour la protection de ses données personnelles figurent le contrôle et la transparence. En effet, comme vu précédemment, la préoccupation pour la protection de ses données personnelles est définie sous l'angle du contrôle d'accès aux informations personnelles : le contrôle de l'accès à soi-même (Altman, 1975), le contrôle de ses limites personnelles et de ses contacts avec les autres (Pedersen, 1997), la réclamation des individus, des groupes, des institutions pour déterminer quand, comment et dans quelle mesure les informations personnelles sont communiquées aux autres (Westin, 1967). Ainsi, des technologies et des réglementations sont mises en place pour permettre à chacun de contrôler la divulgation de ses informations, mais nous n'avons pas toujours le contrôle de nos données. C'est pourquoi l'autorisation du partage d'informations repose sur un « contrat social », i.e., des attentes conventionnelles et implicites entre personnes et/ou organisations sur les informations personnelles qui peuvent être partagées et/ou utilisées. Ce contrat social repose sur une transparence dans l'échange : la théorie du contrat social suggère que la transparence garantit un échange équitable d'informations entre les consommateurs et les organisations (Culnan & Bies, 2003) et les consommateurs tiennent compte de la transparence dont les organisations font preuve dans les échanges (Donaldson & Dunfee, 1994). Par voie de conséquence, la transparence diminue la perception de violation de vie privée (Martin et al., 2017) et rend les consommateurs plus disposés à divulguer des informations (Son & Kim, 2008).

1.3.2. Confiance et vulnérabilité

De ce principe d'échange basé sur un équilibre entre contrôle et transparence, découlent deux autres notions : la confiance et la vulnérabilité. La transparence et le contrôle sont fortement associés à la confiance (Swani et al., 2021), et une relation de transparence sur le long terme renforce la confiance du consommateur et son engagement (Culnan & Bies, 2003). Par ailleurs, « *La vie privée, dans son ensemble ou en partie, représente le contrôle des transactions entre une ou plusieurs personnes et d'autres personnes, dont le but ultime est de renforcer l'autonomie et/ou de minimiser la vulnérabilité* » (Margulis, 1977, p.10). Cet aspect de

vulnérabilité est d'autant plus important dans le contexte d'usage et de collecte de données personnelles actuel, et face à la croissance exponentielle du nombre de violations de données personnelles, au point où Martin, Borah & Palmatier (2017) se demandent si la vie privée existe encore et ont proposé de reconceptualiser *l'information privacy concern* autour du concept de vulnérabilité. En effet, alors que la capacité de se retirer et de s'isoler est un mécanisme essentiel de protection psychique et d'équilibre personnel, les difficultés à se retirer que présentent les environnements numériques et la probabilité forte de subir des dommages rendent les consommateurs de plus en plus vulnérables. Martin et al. (2017) proposent différents degrés de vulnérabilité, que nous représentons sous forme de pyramide⁷⁰ (cf. Figure 8).

Figure 8 : Pyramide des degrés de vulnérabilité (Martin, Borah & Palmatier, 2017)



Nous pensons qu'il est important de privilégier les notions de confiance et de vulnérabilité (que les variations culturelles permettraient peut-être de mieux éclairer), et qui sont liées aux questions de sécurité. Nous faisons écho aux appels de certains chercheurs qui rappellent les notions de sécurité, de confiance, de dignité, qui sous-tendent historiquement le droit à la vie privée (tel que défini dans la constitution universelle des Droits de l'homme).

En effet, Solove & Hartzog (2022) appellent à une reconceptualisation de la préoccupation pour la protection de ses données personnelles, dont les dimensions seraient élargies : « *Le respect*

⁷⁰ Mise en forme utilisée par Kelly Martin dans une conférence le 03.05.2021.

de la vie privée est (ou du moins devrait être) bien plus que la simple réalisation des préférences personnelles des gens quant à l'accès à leurs données. La vie privée est une question de confiance, de pouvoir, de dignité et d'autonomie collective pour définir les conditions préalables à l'épanouissement humain. Dans un sens plus large, la vie privée concerne toutes les règles qui régissent nos informations personnelles. De même, la politique de sécurité des données ne peut échapper à un réseau de décisions fondées sur des valeurs, car elle nécessite elle aussi des compromis » (p.135). Aussi, nous ajoutons qu'une reconceptualisation en dehors du champ des systèmes d'information pourrait probablement compléter une vision positiviste de la vie privée (à l'aide d'approches plus exploratoires) et mieux tenir compte de l'ensemble du comportement du consommateur.

1.4. Dépendance au contexte qui appelle une reconceptualisation

Une des raisons de la nécessité de reconceptualisation de la préoccupation pour la protection de ses données personnelles vient du fait que **certains chercheurs considèrent que la *privacy* est un concept contextualisé** (e.g., Martin et Murphy, 2017 ; Pavlou, 2011 ; Smith et al., 2011 ; Nissenbaum, 2004 ; Fogues et al., 2017 ; Nissenbaum, 2010), i.e., dépendant du contexte dans lequel il entre en jeu, et dont les dimensions doivent être reconsidérées régulièrement : « *la dimensionnalité [de la vie privée] n'est ni absolue ni statique, car les perceptions des défenseurs, des consommateurs et des chercheurs peuvent évoluer avec le temps* » (Smith et al., 1996, p.190). Le concept de préoccupation pour la protection de ses données personnelles ne pourrait donc être défini de façon générale.

Plus précisément, le contexte est défini selon des cadres sociaux caractérisés par des activités, des rôles, des relations, des normes, des règles, des valeurs ou des objectifs (Nissenbaum, 2010). Le cadre de l'intégrité contextuelle de Nissenbaum (2004), qui est le travail théorique le plus significatif sur ce sujet, indique que le contexte est défini par trois paramètres : les acteurs (sujet, expéditeur, destinataire), les attributs (types d'information) et les principes de transmission (contraintes et normes sous lesquelles l'information circule). Tout changement de ces paramètres fait changer le contexte. Ce qui est acceptable dans un contexte défini par certaines normes ne l'est plus dans un autre contexte défini par d'autres normes : le concept de préoccupation pour la protection de ses données personnelles doit, de ce fait, être redéfini.

Cette pensée vient à l'encontre de celle qui sous-tend les réglementations en vigueur (RGPD, CPRA) selon lesquelles une donnée est violée quand l'information est collectée, stockée et/ou utilisée à l'encontre du souhait du consommateur, en dehors de toute considération contextuelle, qui rendrait une violation plus ou moins acceptable..

Ainsi, les conceptualisations initiales de préoccupations relatives à la vie privée sur Internet se sont surtout concentrées sur le contrôle (possible à l'époque) de la diffusion des informations personnelles et sur les interactions avec les vendeurs en ligne, dans un contexte traditionnel de commerce électronique. Les besoins en matière de protection de la vie privée en ligne d'aujourd'hui ont beaucoup évolué. Par exemple (cf. Tableau 17) :

- Constatant un manque de conceptualisation de la préoccupation pour la protection de ses données personnelles dans le contexte des interactions en ligne avec des pairs, Zhang et al. (2022) proposent le concept de *Peer Privacy Concern*, i.e., le sentiment de maintien de limites personnelles dans les interactions en ligne avec ses pairs, avec quatre dimensions : *information privacy* (reconceptualisé pour mieux prendre en considération la confidentialité du traitement des informations partagées par les pairs), *psychological privacy* (i.e., préoccupations psychologiques relatives à la confidentialité), *communication privacy* (i.e., préoccupations relatives à la confidentialité lors des communications), and *virtual territory privacy* (i.e., préoccupations relatives au territoire virtuel) ;
- De même, Li et al. (2020) ont conceptualisé la *privacy concern for traceable information* (PCTI) dans le cas de l'utilisation des plateformes de partage de scooters. Ces deux recherches mobilisent les dimensions de *interactional privacy* (i.e., capacité des personnes à contrôler leurs rencontres et interactions avec d'autres personnes ; Burgoon et al., 1989) et de *psychological privacy* (i.e., capacité à se protéger contre des intrusions d'autrui dans ses pensées, sentiments, attitudes et valeurs, ce qui est particulièrement nécessaire pour le développement identitaire ; Burgoon et al., 1989). Ces dimensions sont particulièrement importantes dans les nouveaux usages, tels que les réseaux sociaux.

De la même manière, la segmentation des consommateurs selon des critères de vie privée (Westin Privacy Segmentation Index, 1967 ; Westin, 1967) fait l'objet de débats (Kumaraguru & Cranor, 2005; Martin & Nissenbaum, 2016). Le Westin Privacy Segmentation Index propose une segmentation des consommateurs selon un critère classique de préoccupation pour la

protection de la vie privée en trois groupes : fondamentalistes de la vie privée, pragmatiques de la vie privée, et ceux qui ne se soucient pas de la vie privée. Cette segmentation est critiquée : comme le comportement du consommateur en matière de vie privée change en fonction du contexte, cette segmentation devrait intégrer des éléments contextuels et situationnels.

Le constat de la dépendance contextuelle de la préoccupation pour la protection de ses données personnelles a trois conséquences pour notre recherche. Premièrement, les pratiques des entreprises répondent à des micronormes dépendantes du contexte tout en respectant des principes sociétaux (hyper-normes) tels que la fidélité, la sécurité, le consentement, la notification et la sortie (Donaldson & Dunfee, 1994 ; Martin, 2012). La perception et la compréhension des violations de données personnelles ne dépendent pas uniquement de l'intentionnalité de l'entreprise et de la sensibilité des données, mais du contexte dans lequel la violation se produit. En d'autres termes, la protection de la vie privée et des données personnelles repose sur une vision normative de la vie privée, sur une vision contractuelle de la vie privée spécifique à la situation d'échange et sur des normes dépendantes du contexte (Martin, 2016; Martin, 2012).

Deuxièmement, une étude récente (Grosso et al., 2020) soutient l'importance d'adopter une approche multi-niveaux (macro, méso et micro) pour examiner les intentions en matière de protection de la vie privée et mieux les comprendre, du fait de la dépendance au contexte des intentions des consommateurs en matière de protection de la vie privée.

Troisièmement, si la *privacy* est dépendante du contexte, nous pouvons nous interroger sur sa dépendance culturelle également, et sur la nécessité de la même manière à intégrer des dimensions qui permettent d'une couvrir toute l'étendue culturelle nécessaire.

En somme, le constat de la dépendance contextuelle du souci de contrôle de ses données personnelles met en lumière la nécessité d'une approche multi-niveaux et faisant varier les effets culturels.

*

Nous avons montré que *l'information privacy concern* est classiquement définie comme la capacité à contrôler l'usage et le partage de ses informations personnelles. C'est pourquoi le concept de protection de la vie privée repose sur des dimensions clés de contrôle, de transparence et de confiance. Or dans un contexte d'usage et de collecte explosifs de données personnelles : (i) il existe une perte de contrôle et plus une préoccupation de protection de ses données personnelles, (ii) *l'information privacy concern* fait l'objet de nombreuses reconceptualisations pour prendre en considération les aspects spécifiques à chaque contexte, (iii) la dimension de vulnérabilité prend une importance croissante.

Regardons désormais les grandes approches théoriques en matière de protection de la vie privée.

2. Psychologie de la préoccupation pour la protection de la vie privée

Dans cette partie, nous montrons que la préoccupation pour la protection de la vie privée et de ses données personnelles a été étudiée à trois niveaux d'observation, sociétale, économique et psychologique (2.1). Nous nous intéressons en particulier au troisième niveau et précisons les angles théoriques mobilisés pour éclairer la compréhension de la psychologie de la vie privée (2.2), au sein duquel nous détaillons le modèle APCO, ainsi que les évolutions dont il a fait l'objet pour mieux prendre en compte le manque de rationalité dans les arbitrages paradoxaux en matière de protection de la vie privée.

2.1. Trois niveaux d'observation (économique, sociétal et psychologique) de la protection de la vie privée

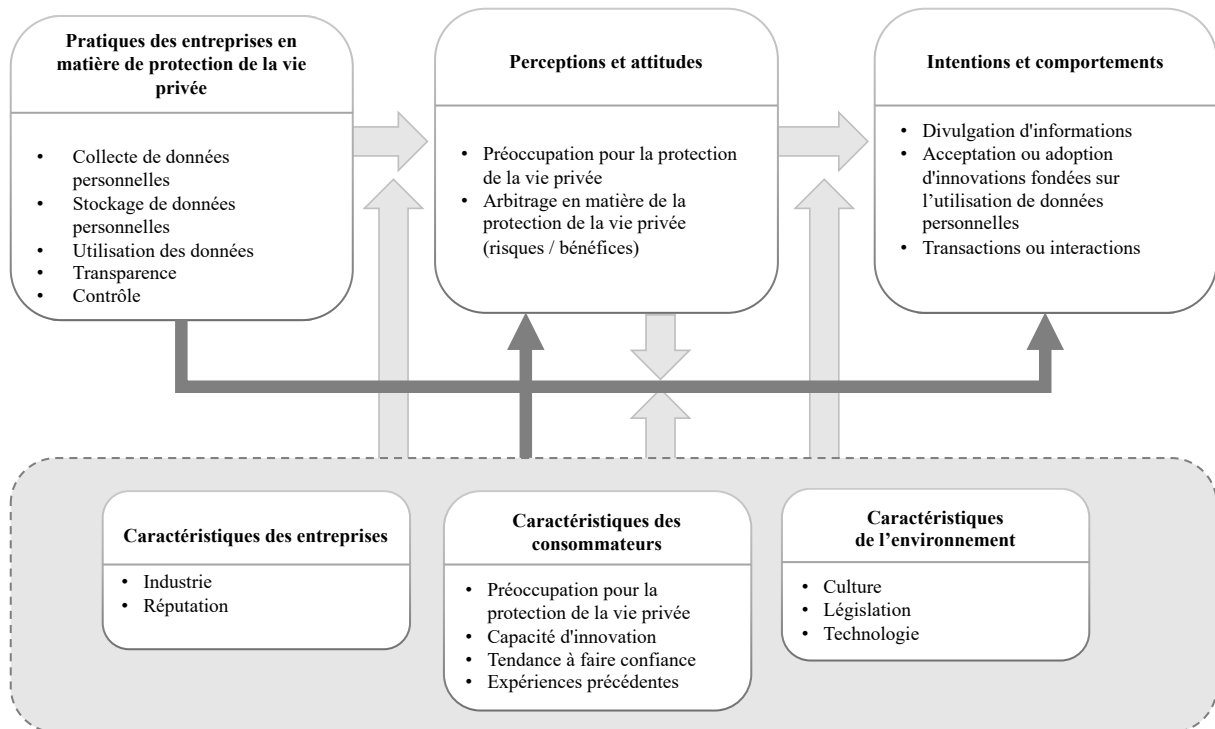
Les recherches portant sur la préoccupation pour la protection de ses données personnelles ont dans le passé étudié trois axes (Martin & Murphy, 2017; cf. Tableau 18) : la vie privée dans la société, la psychologie de la vie privée et l'économie de la vie privée. Ces trois axes correspondent à trois niveaux d'observation : macro (institutionnel), micro (psychologique) et méso (organisationnel).

Tableau 18 : Trois niveaux d'observation de la privacy (Martin & Murphy, 2017)

Niveaux	Description	Théories mobilisées / remarques
La vie privée dans la société	Cadres éthiques	Normative vs. descriptive Utilisation discutable des technologies
	Variations globales	Préférences cross-culturelles Variations réglementaires transnationaux
	Implications juridiques et politiques	Réglementation volontaire ou gouvernementale Intervention en cas d'atteinte à la vie privée
La psychologie de la vie privée	Antécédents à la protection de la vie privée des consommateurs	Souci pour le contrôle de ses données personnelles Vulnérabilité du consommateur Différences individuelles et personnalité
	Facteurs favorisant de protection de la vie privée des consommateurs	Confiance organisationnelle Valeur perçue de la personnalisation Contrôle du consommateur Transparence des données
	Résultats en matière de protection de la vie privée des consommateurs	Intention d'achat Souhait de se dévoiler Clics publicitaires, falsification d'informations Bouche-à-oreille négatif Changement de fournisseur
L'économie de la vie privée	Non-respect de la vie privée	Violations de données personnelles Vol et usurpation d'identité Actions hypercompétitives
	Résultats organisationnels	Performance de l'entreprise Capital-marque Relations avec le client / consommateur Autorégulation de la vie privée <i>Privacy</i> en tant que stratégie

Ces trois niveaux d'observation sont liés : le cadre juridique ou politique amène les organisations à adopter de nouvelles contraintes et procédures, les réglementations augmentent la sensibilité des consommateurs, leurs pratiques professionnelles leur permettent de monter en compétence, ils peuvent alors devenir plus exigeants vis-à-vis des autorités de protection, etc. Il s'agit d'un cercle vertueux ! La littérature a alors étudié les différents effets comme indiqué sur la Figure 9. Les pratiques des entreprises impactent les perceptions et attitudes des individus et par conséquent leurs intentions et comportements, le tout étant influencé par les caractéristiques de l'entreprise, de l'environnement et des consommateurs eux-mêmes.

Figure 9 : État de la littérature en matière de protection de la vie privée du consommateur (Beke et al., 2018)



Les violations de données personnelles sont essentiellement étudiées dans le cadre de l'économie de la vie privée (cf. Tableau 18), laissant de côté une meilleure compréhension du comportement psychologique ou sociologique de réponse des individus. La culture est considérée comme un facteur macro (Smith et al., 2011), minimisant une meilleure compréhension de ses dimensions individuelles et psychologiques. Notre recherche propose de mieux explorer cet aspect. Ceci nécessite au préalable de faire état de la littérature sur la psychologie de la vie privée.

2.2. Cadre général de la psychologie de la vie privée

Le développement des technologies a amené les individus à prendre de nombreuses décisions en matière de protection de leur vie privée au quotidien. Le souci pour la protection de la vie privée joue un rôle central dans le comportement en ligne des consommateurs (comme les achats en ligne ou les contributions aux communautés), mais également des citoyens (à travers les nombreux services publics en ligne). Ce comportement en ligne est influencé par des antécédents et résulte de l'interaction de facteurs psychologiques, facilitateurs ou inhibiteurs (Dinev et al., 2006). Cette approche se fonde essentiellement sur le modèle APCO que nous précisons ci-après. À partir de celui-ci, plusieurs théories ont été mobilisées : nous les présentons. Et, nous identifions quelques voies de recherche.

2.2.1. Modèle APCO

Les recherches sur la formation des préoccupations des consommateurs en matière de confidentialité des informations sont principalement basées sur le modèle APCO (Dinev et al., 2015; Smith et al., 2011) : **Antecedents – Privacy Concern – Outcomes**. Les antécédents sont précisés ci-dessous. Les résultats (*outcomes*) sont l'achat, la divulgation, la protection, la loyauté, la confiance, l'acceptation d'une technologie ou d'un service.

Le modèle APCO synthétise les précédentes recherches en plaçant le souci pour le contrôle de ses données personnelles au centre du modèle, et met en évidence 3 types d'antécédents (Miltgen, 2009; Miltgen & Peyrat-Guillard, 2014) : individuels, situationnels (contextuels) et macro. Plus précisément :

- Les facteurs individuels peuvent être sociodémographiques (âge, sexe, CSP), psychologiques, cognitifs (expérience, connaissance), idéologiques (Dinev et Hart, 2006) ;
- De nombreux facteurs contextuels peuvent orienter les préoccupations en matière de vie privée : les acteurs impliqués dans le traitement des données (Yun et al., 2019), la technologie utilisée, la sensibilité des informations collectées (Mothersbaugh et al., 2012) ;
- Les facteurs macro sont des variables généralement considérées à un niveau national, tels que la culture, le climat, le taux d'équipement et la réglementation.

Smith et al. (2011) a regretté que ces antécédents aient été étudiés indépendamment les uns des autres. De plus, le modèle a été revu ensuite par Dinev et al. (2015), critiquant le fait que le modèle APCO originel étudie les réponses attitudinales et comportementales résultant d'évaluations rationnelles, informées et délibérées. Or, des recherches issues de l'économie comportementale et de la psychologie identifient 3 limites auxquelles se heurtent les individus cherchant à préserver leur vie privée tout en maximisant leur utilité tirée de l'échange (i.e., *privacy calculus*, cf. infra) (Acquisti, 2004) : l'incomplétude de l'information (l'individu ne dispose de quasiment aucune information lui permettant de juger convenablement de la transaction), la rationalité limitée (capacités cognitives limitées dues à une grande quantité d'informations à traiter en très peu de temps) et les distorsions psychologiques (e.g., les biais d'optimisme). Ainsi, Dinev et al. (2015) proposent un modèle APCO revisité qui distingue les *high-effort cognitive responses*, qui sont présentes dans le modèle APCO initial, et les nouvelles *low-effort cognitive responses* issues des recherches en économie comportementale et en psychologie. Les *low-effort cognitive responses* comprennent (i) les aspects cognitifs, affectifs, ainsi que les contraintes temporelles, (ii) les biais heuristiques et périphériques.

Malheureusement dans le modèle APCO revu, la culture est toujours identifiée parmi les facteurs macro, tout en soulignant que « *les sociétés ou les cultures ont certainement des attentes sur les personnes à qui faire confiance ou les pertes à éviter qui vont conduire les actions liées à la vie privée dans ces contextes plus larges* » (Dinev et al., 2015, p.651).

Cependant, il est encore important d'éclairer les mécanismes psychologiques d'arbitrage face à des choix qui impliquent la protection de la vie privée. À ce titre, des recherches récentes mettent en avant le rôle de la distance psychologique, qu'il nous semble toujours nécessaire d'explorer. Nous l'expliquons dans le paragraphe suivant. Par ailleurs, plusieurs recherches montrent que les préoccupations des utilisateurs en matière de protection de la vie privée ne « sont parfois qu'un faible prédicteur des décisions en la matière » (Li et al., 2022, p.4), ainsi d'autres antécédents doivent être pris en considération, que nous verrons ultérieurement.

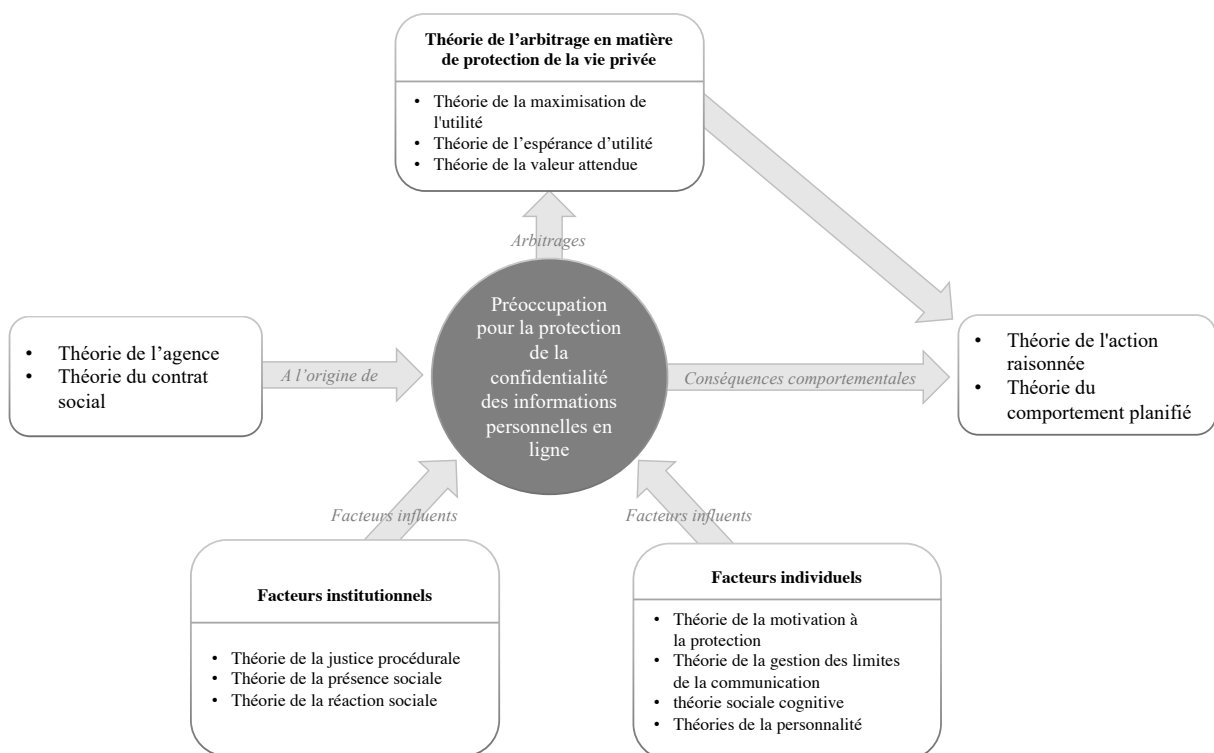
2.2.2. Grandes théories en psychologie de la vie privée

Plusieurs théories ont été mobilisées pour expliquer la psychologie de la vie privée et la formation du comportement en matière de protection de la vie privée des individus (cf. Figure 10 ci-dessous ; Li, 2012). Ces cadres théoriques sont classés en 4 catégories :

- Les théories qui expliquent les antécédents à la préoccupation pour la vie privée,
- Celles qui mettent en lumière les compromis et arbitrages,
- Celles qui expliquent les conséquences comportementales,
- Celles qui identifient les facteurs influenceurs, institutionnels ou individuels.

À cela peuvent s'ajouter d'autres théories pour expliquer la formation d'un cadre global de protection de la vie privée (*institutional theory, ressource-based view*).

Figure 10 : Théories mobilisées dans les recherches en préoccupation pour la protection de la vie privée (Li, 2012)



Les théories présentes dans la Figure 10 sont détaillées en Annexe 4.

Notre thèse s'intéresse aux effets culturels sur le comportement de réponse face à une violation de données personnelles à un niveau macro, méso et micro. En nous référant au schéma de la Figure 10, les théories que nous mobilisons dans le cadre de notre thèse se positionnent à chacun de ces trois niveaux d'observation :

- Le niveau macro s'intéresse aux antécédents et facteurs institutionnels influents,
- Le niveau méso s'intéresse aux facteurs individuels influents (avec la nécessité d'ajouter les effets sociétaux) et aux conséquences comportementales,
- Le niveau micro s'intéresse aux arbitrages.

Dans ce contexte, nous enrichissons des théories déjà existantes avec une nouvelle approche théorique, et en précisons les voies possibles. _

2.2.3. *Voies de recherche théorique*

Premièrement, il a été montré que la préoccupation pour la protection de la vie privée était un concept de « haut niveau » (Hallam & Zanella, 2017), distant and abstrait (Bandara et al, 2018). De plus, Bandara et al. (2021) valident empiriquement le concept de distance psychologique (Trope & Liberman, 2010) avec la préoccupation pour la protection de la vie privée, et soulignent d'une part que la distance psychologique affaiblit la relation entre préoccupations en matière de vie privée et comportement défensif, et d'autre part que les personnes autonomes et compétentes en matière de vie privée (*empowered*) ne sont pas influencées dans leurs intentions comportementales par la distance psychologique avec la préoccupation pour la protection de la vie privée. Enfin, la théorie de la distance psychologique permet également d'expliquer dans quelle mesure la satisfaction à l'égard des usages Internet est à l'origine du paradoxe de la personnalisation et de la protection de la vie privée (Cloarec et al., 2022). Ces recherches servent de bases intéressantes pour de futures explorations.

Deuxièmement, il est étonnant qu'aucune approche théorique sociologique n'ait été mobilisée.

*

Alors que la protection de la vie privée est étudiée à trois niveaux, sociétal, économique et psychologique, (i) les violations de données personnelles sont étudiées avec un angle économique, et non psychologique ou sociologique, (ii) la culture est considérée comme un facteur macro, et non sociétale ou psychologique. Nous avons, pour cela, détaillé les recherches en psychologie de la vie privée : au fur et à mesure du temps, les arbitrages individuels en matière de vie privée et de protection des données personnelles sont de moins en moins rationnels. La protection de la vie privée est un concept abstrait : une meilleure compréhension des niveaux de représentation de la protection de la vie privée mobilisant la théorie de la distance psychologique permettra d'éclairer ces questions.

3. Autres facteurs influençant les comportements de protection des données

Plusieurs recherches mettent l'accent sur le fait que les préoccupations des utilisateurs en matière de protection de la vie privée ne « *sont parfois qu'un faible prédicteur des décisions en la matière* » (Li et al., 2022, p.4) et des comportements réels : d'autres antécédents doivent alors être pris en considération. En particulier, face à une violation de ses données personnelles : sais-je comment répondre et suis-je capable de répondre ? que me préconise de faire mon entourage ?

Dans cette partie, nous précisons le rôle de la pression sociale, à travers les bénéfices sociétaux des réponses et les normes subjectives (3.1) et de l'auto-efficacité (3.2).

3.1. Rôle de la pression sociale

3.1.1. Bénéfices sociétaux

Son et Kim (2008) dans leur modèle de réponses pour la protection de la vie privée (cf. Figure 12) identifient les bénéfices sociétaux perçus de la plainte, i.e., la mesure selon laquelle un internaute estime que le fait de se plaindre d'une atteinte à la vie privée profitera à d'autres internautes en les empêchant d'être victimes de la même chose, comme antécédent important au comportement de plaintes.

3.1.2. Normes subjectives

Par ailleurs, parmi les facteurs influençant le souci de vie privée (cf. Tableau 19), certains aspects tels que les normes subjectives ou l'auto-efficacité n'ont pas été suffisamment mobilisés (Li, 2012).

Tableau 19 : Facteurs influençant le souci de vie privée (Li, 2012)

Facteurs qui augmentent le souci de vie privée	Facteurs qui diminuent le souci de vie privée
La perception des risques et vulnérabilité, L'anxiété informatique, L'expérience antérieure d'atteinte à la vie privée Les traits de personnalité tels que la conscience sociale, le caractère consciencieux, l'ouverture à l'expérience, la méfiance cynique, la paranoïa, la critique sociale, le besoin psychologique de vie privée	La réputation du site web, Les interventions des vendeurs telles que les politiques de confidentialité, l'informativité des sites Web et la présence sociale, La sensibilité à l'information, L'auto-efficacité et la contrôlabilité, Les personnalités telles que l'agréabilité.

Les normes subjectives, i.e., les perceptions des individus de la pression sociale, représentée par ce que pensent les proches du comportement prévu ou entrepris (Ajzen, 1991), jouent un rôle déterminant dans la personnalisation des services sur Internet (Lee & Park, 2009). Notamment la pression sociale à utiliser certains services personnalisés amène à communiquer ses informations personnelles (Aguirre et al., 2015).

Par ailleurs, les modèles TAM (Technology Acceptance Model) et UTAUT, qui intègrent les normes subjectives, sont largement utilisés pour l'acceptation des nouvelles technologies et de l'intelligence artificielle (IA) :

- Le modèle TAM (Davis, 1989) suggère que les intentions comportementales sont influencées par (i) l'utilité perçue et la facilité d'utilisation perçue et (ii) des variables externes telles que les normes subjectives ;
- Le modèle UTAUT (Venkatesh et al., 2003) avance que les intentions comportementales sont influencées par (i) les attentes en matière de performance, (ii) les attentes en matière d'effort, (iii) l'influence sociale (proche de la dimension de *subjective norms*, i.e., « les personnes qui influencent mon comportement pensent que je devrais utiliser... », (iv) les conditions facilitatrices.

De plus, Mariani et al. (2022) recommandent pour éclairer les questions d'adoption des outils d'intelligence artificielle par les consommateurs d'intégrer dans le modèle UTAUT la *protection motivation theory* (PMT). La PMT indique que l'acceptation d'une technologie est influencée par une évaluation de l'adaptation (composée de *response efficacy*, *response cost* et *self-efficacy*) et de la menace (composée de la vulnérabilité perçue et la sévérité perçue).

L'ensemble de ces dimensions semblent pertinentes au regard des comportements de réponse face à une violation de ses données personnelles.

Enfin, certaines orientations culturelles (i.e., collectivisme et orientation à long terme) privilégient l'adoption de comportements d'achat écologiques en raison de normes subjectives fortes (Nguyen et al., 2017). « *Les normes sociales sont des déterminants plus forts du comportement prévu pour les individus qui épousent des valeurs culturelles féminines et de fort contrôle de l'incertitude* » (Srite & Karahanna, 2006, p.679).

3.2. Auto-efficacité

L'auto-efficacité, ou *self-efficacy*, fait référence à la croyance d'un individu en sa capacité d'exécuter les comportements nécessaires à la réalisation de performances spécifiques (Bandura, 1977). La *self-efficacy* a été adaptée à la privacy, avec le concept de *privacy self-efficacy*, i.e., l'évaluation que chacun fait de sa capacité à protéger sa vie privée en ligne (Mamonov & Benbunan-Fich, 2018). La *privacy self-efficacy* s'avère avoir un impact négatif sur la préoccupation relative à la vie privée. De plus, il s'agit d'une dimension souvent mentionnée théoriquement comme jouant un rôle dans les réactions face à des menaces, malgré un manque d'évidence empirique et le fait que l'*efficacy* n'ait pas de lien avec la *privacy concern* (Adhikari & Panda, 2018). Les modèles TAM et UTAUT sont utilisés dans des recherches récentes dans l'adoption de la blockchain (Toufaily et al., 2021) et des *chatbots* (Balakrishnan et al., 2022). Notamment Balakrishnan et al. (2022), dans le cas des *chatbots*, introduit une nouvelle dimension au modèle UTAUT : la social self-efficacy, i.e., la croyance individuelle dans sa capacité à accomplir une tâche ou à avoir un comportement donné dans les relations sociales avec succès.

Synthèse de la section sur la préoccupation pour la protection de la vie privée

La préoccupation pour la protection des données personnelles repose sur le droit des individus de contrôler l'accès et l'usage de leurs données personnelles, et sur un principe de contrat social entre un individu et une entreprise qui collecte les données. Ainsi les proxys utilisés pour évaluer la préoccupation pour la protection des données personnelles sont définis autour de dimensions de contrôle et de transparence.

La préoccupation pour la protection des données personnelles intervient dans les arbitrages institutionnels et réglementaires (macro), économiques et organisationnels (méso), psychologiques (micro).

Dans un contexte d'usage et de collecte explosive de données personnelles, la préoccupation pour la protection des données personnelles fait l'objet de débats, car est une notion abstraite donc prise artificiellement en considération dans les arbitrages des individus, générant des situations paradoxales entre un souci de protection déclaré et un comportement réel, avec un impact sur la vulnérabilité du consommateur (d'autant plus importante dans le cas de violations de données personnelles). Par conséquent, la préoccupation pour la protection des données personnelles fait l'objet de nouvelles conceptualisations et des recherches explorent le rôle de la distance psychologique avec les risques liés à la vie privée.

Une meilleure compréhension des intentions comportementales face à une violation de données personnelles et des mécanismes reliant valeurs et réponses implique de mieux comprendre le rôle la préoccupation pour la protection des données personnelles, qui peut être un antécédent mineur face à d'autres facteurs sociétaux (e.g., pression sociale) dans les réponses apportées.

Section 2. Réponses des consommateurs insatisfaits

“I have never given up looking for new solutions to political problems”
(Hirschman, 1998, p.87)

Nous avons fait le constat dans le chapitre introductif que les recherches sur le comportement de réponse face à une violation de données personnelles, et en particulier en marketing, manquent. Cette seconde partie a pour objectif de faire état des recherches sur le comportement de réponses des consommateurs insatisfaits, afin d’éclairer nos réflexions sur le comportement de réponses face à une violation de données personnelles : quels sont les antécédents qui génèrent une réponse ? Et pour quelles raisons une personne cherche-t-elle à se plaindre ? Quel processus ce comportement va-t-il suivre ? Existe-t-il déjà des recherches qui portent sur le comportement de réponses pour la protection de la vie privée ? Dans une première partie, nous présenterons en synthèse la littérature en comportement de plainte du consommateur (*consumer complaint behaviour - CCB*). Dans une deuxième partie, nous exposerons les recherches portant sur les réponses pour la protection de la vie privée, et y porterons un regard critique.

1. Comportement de plainte du consommateur

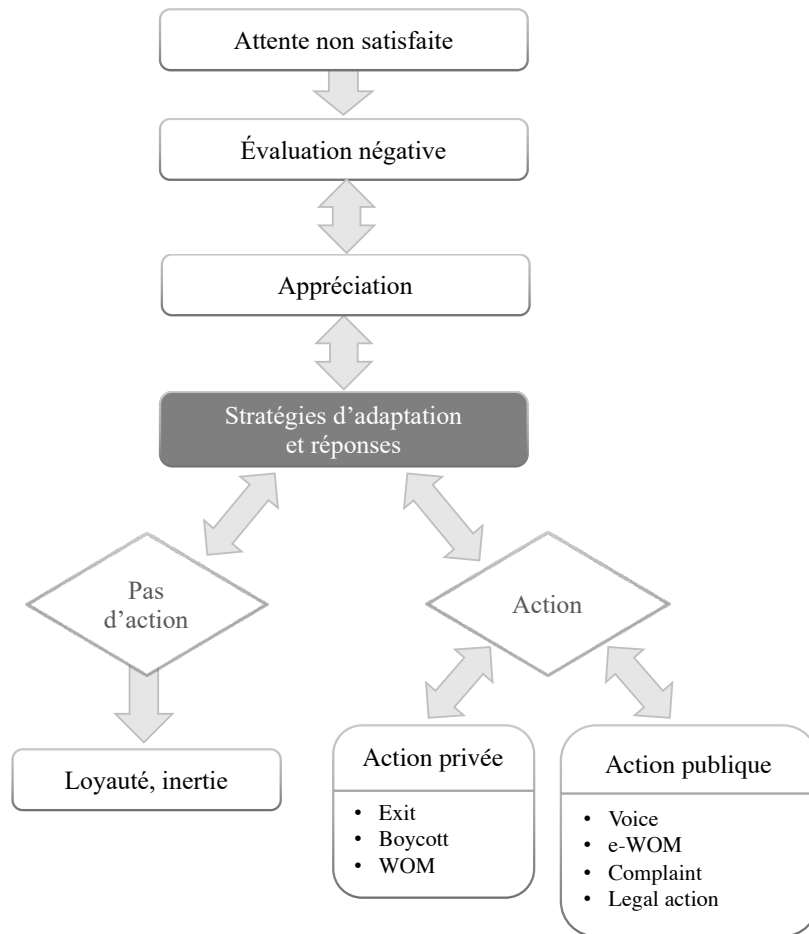
Cette partie a pour objectifs de faire une présentation synthétique du large champ de recherche en CCB (1.1), puis de détailler les étapes du processus de comportement de plainte (1.2) et les antécédents au comportement de plainte (1.3).

1.1. Étapes du processus de comportement de plainte du consommateur

La littérature en marketing s'est beaucoup intéressée depuis 40 ans au comportement de plainte des consommateurs (Day & Landon, 1977; Singh, 1988), dans un cadre large de la gestion des relations clientèle, en particulier dans le cas des services (e.g., Bach & Kim, 2012; Gyung Kim et al., 2010; Ro, 2015), du tourisme (e.g., Dimanche & Havitz, 1995) ou de l'hôtellerie (e.g., Jahandideh et al., 2014; Ngai et al., 2007). Le comportement de plainte du consommateur connaît des évolutions récentes. Internet et les réseaux sociaux offrent au consommateur de nouvelles possibilités d'expression et augmentent la probabilité d'un comportement de plainte en ligne (N'Goala et al., 2019; Siret & Sabadie, 2022).

Le comportement de plainte des consommateurs, ou *consumer complaint behaviour*, est défini comme la conséquence d'un acte de consommation (d'un produit ou d'un service) ayant généré une forte insatisfaction pour le consommateur, ayant un impact psychologique fort et ne pouvant être oubliée (Day et al., 1981) ou comme la tentative du client de modifier une situation insatisfaisante (Fornell & Wernerfelt, 1987). Auparavant, les causes d'une insatisfaction étaient des questions de prix, d'inconvénients de produits, de défaillances de service ou des problèmes d'éthique (Keaveney, 1995). Bien que ce champ se soit nommé *consumer complaint behaviour*, les réponses des consommateurs face à une insatisfaction peuvent être diverses et non limitées à la plainte, comme nous le verrons page suivante.

Le comportement de plainte du consommateur procède en trois étapes : l'évaluation négative de l'acte de consommation, l'appréciation, les stratégies d'adaptation et réponses. Ce processus de réponse à une attente non satisfaite est présenté dans la Figure 11 ci-après.

Figure 11 : Processus de réponse à une attente non satisfaite

1.2. Étapes du processus de comportement de plainte du consommateur

1.2.1. Étape 1 de la plainte : l'évaluation négative d'une situation

L'évaluation négative d'une situation (de consommation) correspond à une attente non satisfaite de la performance attendue d'un produit ou d'un service (Brady et al., 2005), d'un échec du service ou d'un échec dans les réponses apportées à ces échecs (Keaveney, 1995). Il s'agit plus particulièrement d'une évaluation entre les attentes et le niveau de service, étudiée notamment à l'aide de l'*expectation-disconfirmation theory* (Stauss et al., 2005). Cela aboutit à une situation d'insatisfaction. Néanmoins, l'insatisfaction n'est pas le seul facteur initiateur de la plainte (Crié, 2003) : des facteurs psychologiques (e.g., la frustration, le stress), des facteurs individuels (e.g., la loyauté, les expériences passées, la capacité à détecter les défaillances) et d'autres facteurs interviennent dans le processus de plainte en parallèle de l'insatisfaction.

1.2.2. *Étape 2 de la plainte : l'appréciation cognitive de la situation*

Deuxièmement, l'appréciation est un processus cognitif et émotionnel (Lazarus, 1966, 1991) composé de phases simultanées ou successives (Gyung Kim et al., 2010), qui portent sur l'échec lui-même et le stress généré (d'autant plus important s'il concerne l'ego, comme la vie privée), et sur les capacités de prise en charge et d'attribution. La théorie de l'attribution indique notamment que le jugement de responsabilité du client suit un processus cognitif en fonction de la perception du client d'un résultat et de la conformité de ce résultat aux attentes (Hamilton, 1978). Enfin, la dissonance cognitive, le sentiment de justice (Sabadie et al., 2006) et les émotions (Stephens & Gwinner, 1998) jouent un rôle très important dans cette deuxième étape d'appréciation.

1.2.3. *Étape 3 de la plainte : les stratégies d'adaptation et de réponse*

Troisièmement, les consommateurs développent des stratégies d'adaptation et de réponses dans l'objectif de réduire le niveau d'insatisfaction et le stress causé par l'insatisfaction. Ces stratégies peuvent varier selon l'objectif (centré sur le problème, sur les émotions ou sur l'évitement), certains antécédents saillants et les possibilités (e.g., les coûts, les efforts, la probabilité perçue de succès). À cette étape, l'individu fait une évaluation « coûts vs. bénéfices » qui a été éclairée par la *prospect theory* (indiquant que l'individu fait des choix entre alternatives, risques et résultats attendus de la plainte; Kahneman & Tversky, 1979) ou l'*equity theory* (indiquant que les attitudes et les comportements sont influencés par l'évaluation des efforts nécessaires et la récompense escomptée ; Austin & Walster, 1974).

Les consommateurs ont trois options possibles : *exit* (i.e., la rupture de toute relation avec l'entreprise), *voice* (i.e., l'expression de l'insatisfaction) et *loyalty* (i.e., ne prendre aucune mesure) (Hirschman, 1970). La théorie d'Hirschman repose essentiellement dans le choix entre *exit*, qui est un choix économique car il présuppose l'existence d'offre alternative, et *voice*, qui est un choix politique car il a pour objectif de modifier l'existant.

Parmi ces options, la *loyalty* ne doit pas être comprise comme une absence d'engagement, mais comme une résignation face à l'absence d'alternative. L'option de loyauté, ou d'inertie, était auparavant la plus fréquente et un grand nombre de clients mécontents se taisaient (Crié, 2003). Or les réseaux sociaux, les blogs et les avis en ligne (type TripAdvisor) offrent de nouveaux

modes d'expression, qui sortent d'un cadre face-to-face, et qui favorisent l'expression du mécontentement et de l'insatisfaction.

Face à la défaillance d'une entreprise, deux possibilités se présentent : la première est la défection ou *exit*, qui relève de l'économie. En effet, d'autres offres se présentant sur le marché, le jeu de la concurrence intervient. Les consommateurs peuvent donc arrêter d'utiliser le produit ou le service (option de sortie, *exit*), notamment à travers des actions de boycott.

La deuxième possibilité est la prise de parole ou *voice*, qui est une action politique, qu'elle soit un simple « ronchonnement à peine perceptible ou une récrimination violente » (Hirschman, 1970, p.27), avec des objectifs de diffusion privée ou publique (Day & Landon, 1977 ; Singh 1988). En effet, si Hirschman (1970) a défini la première taxonomie en CCB (*loyalty exit, voice*), Singh (1988, 1990) a précisé les trois niveaux de *voice* : *voice, private, third party* (i.e., public). Les individus peuvent simplement exprimer leur mécontentement auprès de leur famille et de leurs proches (phénomène de bouche-à-oreille), sans avoir pour objectif d'être connus ou de demander réparation. Ils peuvent s'exprimer de manière plus significative (Lee & Cude, 2012), notamment à travers les blogs et les réseaux sociaux (e-WOM) (Harrison-Walker, 2001), avec pour objectif de rendre publique leur insatisfaction. Cette option d'e-WOM est parfois considérée comme une action privée dans la littérature. Cependant l'e-WOM correspond à une plainte formulée auprès de l'entreprise en ligne et « la plainte en ligne pourrait être interprétée comme une forme de divorce annoncée publiquement » (Grégoire et al., 2009, p.27). Cette plainte revêt alors presque une forme de vengeance, i.e., l'expression d'un sentiment de trahison (Grégoire et al., 2009 ; Grégoire & Fisher, 2008), liée à la violation du lien relationnel entre l'entreprise et ses clients. Enfin les consommateurs peuvent se plaindre auprès de l'entreprise concernée (action publique) en souhaitant une résolution concrète sans dévoilement public. Ils peuvent se plaindre auprès d'un tiers (e.g., associations de protection des consommateurs). Ils peuvent mener des actions en justice (Romanosky et al., 2013), visant une compensation financière.

Les réponses apportées à un acte de consommation insatisfait suivent un processus diachronique (Crié, 2003; Day, 1977) : l'évaluation de la situation par le consommateur évolue dans le temps, selon des facteurs contextuels (e.g., le climat institutionnel et juridique), des facteurs sociaux ou culturels. Les réponses finales ne dépendent pas directement des facteurs initiateurs : c'est pourquoi les flèches sont à double sens dans la Figure 11 ci-avant.

Enfin, la littérature souligne les implications managériales fortes de la prise en charge des plaintes des consommateurs : les entreprises qui répondent de manière appropriée aux insatisfactions et plaintes des consommateurs peuvent transformer de façon positive leur relation avec le client insatisfait et ainsi éviter des effets de contamination (Ballantyne et al., 1995; Knox & van Oest, 2014). De plus, la théorie de la justice souligne la nécessité pour le consommateur que l'insatisfaction a été correctement réparée, cette conscience pouvant beaucoup varier selon les contextes culturels (Lind & Earley, 1992; Murphy-Berman & Berman, 1998).

1.3. Antécédents au comportement de plainte

Les premières recherches en CCB indiquent que les caractéristiques démographiques telles que l'âge, le sexe et l'éducation influencent le comportement des clients en matière de plaintes (Day & Landon, 1977, Warland et al., 1975). Par la suite, l'insatisfaction n'est pas le seul facteur initiateur de la plainte (Crié, 2003), comme nous l'avons déjà indiqué, et d'autres facteurs tels que l'attribution de responsabilité, des facteurs psychologiques (e.g., la frustration, le stress) et les caractéristiques individuelles (e.g., la loyauté, les expériences passées, la capacité à détecter les défaillances) vont intervenir dans le processus en parallèle de l'insatisfaction. En dernier lieu, le choix de passer à l'action et d'apporter une réponse peut dépendre : (i) de facteurs de coût, de compétence et de capacité du consommateur à entreprendre une action de plainte (Gronhaug & Zaltman, 1981) ; (ii) de dimensions de temps, d'efforts, de confiance mutuelle, de possibilité de réactivité, et de pression sociale.

Nous classifions en trois catégories les antécédents au comportement de plainte que nous avons recensés (notamment à partir de Crié, 2003) : les antécédents qui relèvent de l'individu lui-même (facteurs sociodémographique, d'expérience, psychologique, éthique), les antécédents qui relèvent du contexte économique (e.g., structure du marché), et ceux qui relèvent du contexte socioculturel.

Antécédents qui relèvent de l'individu :

- Facteurs sociodémographiques : âge, sexe, niveau socio-éducatif (e.g., Farhangmehr & Silva, 1995) ;
- Facteurs d'expérience : fidélité à la marque (analysée en particulier avec la théorie de l'échange social) , capacité à détecter les différences de qualité et à évaluer la qualité, perception des coûts/avantages (de même avec la théorie de l'équité), apprentissage dépendant des expériences et des résultats passés (de même avec la théorie de l'apprentissage) (Hansen et al., 1997; Jacoby & Jaccard, 1981; Lapidus & Pinkerton, 1995) ;
- Facteurs psychologiques : insatisfaction, frustration perçue, émotions, attribution de responsabilité et injustice perçue, stress dû à des changements dans l'atteinte des objectifs du consommateur, stress dû à une atteinte à l'ego de la personne (humiliation, estime de soi, valeurs éthiques) (Fornell & Westbrook, 1979; Mooradian & Olver, 1997; Stephens & Gwinner, 1998);
- Facteurs éthiques : valeurs éthiques, équité, loyauté (e.g., Cornwell et al., 1991) ;
- Facteurs sociaux : volonté d'agir pour soi mais aussi pour les autres (Barnes & Kelloway, 1980).

Le comportement de plainte peut endosser un rôle social avec la volonté d'agir pour soi mais aussi pour les autres (Barnes & Kelloway, 1980). Se plaindre peut aussi résulter d'influence sociale et de la pression de l'entourage à agir, du degré de stress et d'insatisfaction liés à la compréhension du problème ou encore de capacité à agir (pour des raisons socio-éducatives ou d'expérience).

Antécédents qui relèvent du contexte économique :

- Facteurs économiques : fréquence d'achat et de consommation du produit / service (Andreasen & Best, 1977);
- Facteurs économiques et contextuels propres à la plainte : coût de la plainte (la *transactions costs theory* identifiant 3 dimensions au coût de la plainte : la spécificité, l'incertitude, la fréquence d'échange ; Grønhaug & Gilly, 1991), probabilité de succès et profit attendu, disponibilité de l'information pour aider les consommateurs à faire leurs choix ou à savoir comment se plaindre, performances des services clientèle ;
- Facteurs contextuels : structure du marché, barrières au changement et relation avec l'entreprise (e.g., dans un environnement concurrentiel restreint, les actions verbales

seront la seule action possible pour un consommateur mécontent ; Day et al., 1981; Day & Landon, 1977) ;

- Facteurs régulateurs : climat juridique (confiance institutionnelle), degré de régulation et de contrôle des activités économiques et des pratiques marketing.

Antécédents qui relèvent du contexte socioculturel (Day et al., 1981) :

- Valeurs culturelles (e.g., Chapa et al., 2014; Cornwell et al., 1991; Henthorne et al., 2018; Jahandideh et al., 2014; Liu & McClure, 2001; Wan, 2013; Watkins & Liu, 1996) ;
- Pratiques culturelles : e.g., les habitudes ancestrales de sorcellerie perdurent dans des pays en voie de développement, et priment sur un recours au droit classique ; dans des sociétés accordant de l'importance à la contextualisation dans l'échange, des raisons de non-recours à la plainte peuvent être ignorées et cachées (Ting-toomey & Kurogi, 1998).

Les travaux sur les valeurs culturelles indiquent notamment que les personnes individualistes sont plus susceptibles de réclamer des dommages aux entreprises ou d'exprimer leur mécontentement aux autres (Chapa et al., 2014; Liu et al., 2001; Liu & McClure, 2001). Nous mobiliserons et préciserons ces différentes recherches au fur et à mesure de nos essais.

*

Le comportement de plainte du consommateur est un très large champ de recherche, très étudié, dont nous avons tenté de faire une synthèse aussi complète que possible, en vue de mieux comprendre le comportement de réponse face à une violation de données personnelles. En effet, une violation de données personnelles est la rupture d'un service, une rupture du contrat social et du contrat de confiance qui lie une entreprise et ses clients, générant une attente insatisfaite et un comportement de plainte, voire possiblement un comportement de vengeance (mais dans le cas des violations de données personnelles, la vengeance est-elle possible ?) Nous allons dans la partie suivante préciser les réponses pour protection de la vie privée et des données personnelles.

2. Réponses pour la protection de la vie privée

L'objectif de ce paragraphe est de présenter la taxonomie de Son & Kim (2008) (2.1) et de porter un regard critique sur les modèles existants à l'aune de la littérature en CCB et des évolutions contextuelles actuelles (2.2).

2.1. Taxonomie des réponses pour la protection des données personnelles

Se basant sur la littérature en CCB, Son & Kim (2008) ont proposé une taxonomie séminale des réponses de protection de la vie privée (*information privacy-protective responses* ; cf. Figure 12). La taxonomie de Son & Kim (2008) se structure autour de 6 comportements :

- 2 comportements portant sur la communication d'informations personnelles : refus de divulguer ses informations et divulgation d'informations falsifiées,
- 2 comportements d'actions privées : abandon de service et bouche-à-oreille négatif,
- 2 comportements d'actions publiques : plainte directement aux entreprises concernées ou indirectement aux organisations tierces.

Son & Kim (2008) identifient trois antécédents à ces réponses :

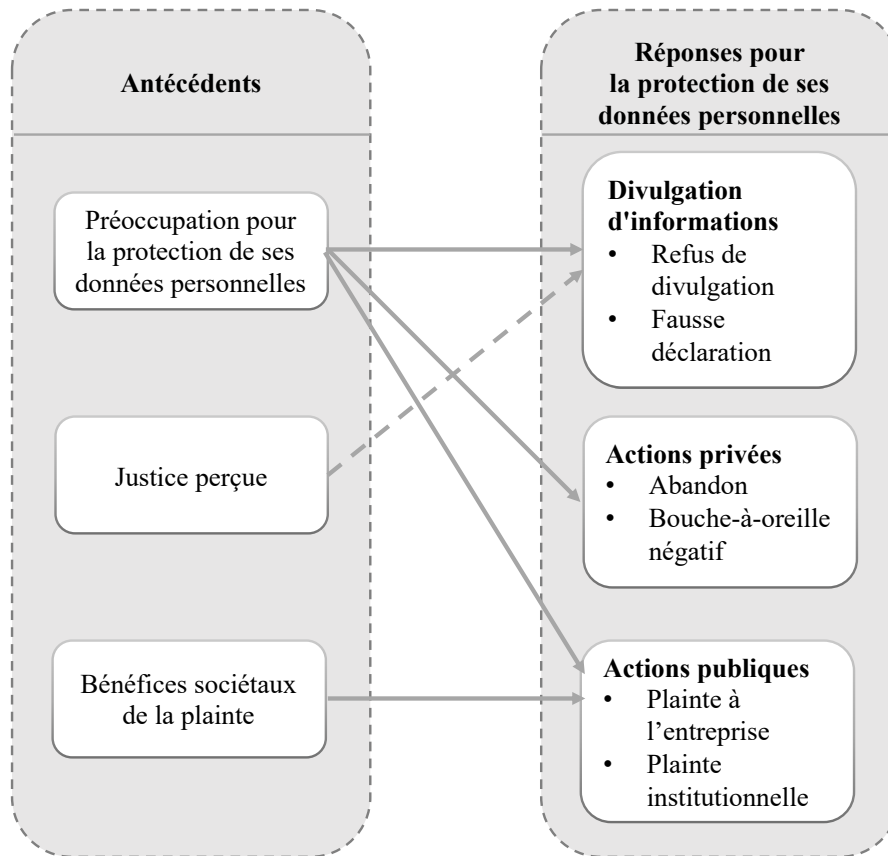
- La préoccupation pour la protection de ses données personnelles ;
- La justice perçue (considérant la justice comme centrale dans tout échange social ; Cialdini 1993 ; et différenciant la justice perçue, distributive, procédurale et interactionnelle⁷¹) ;
- Et les bénéfices sociétaux de la plainte (i.e., le degré selon lequel un utilisateur perçoit que sa plainte pour violation de sa vie privée en ligne pourrait bénéficier à d'autres utilisateurs en leur évitant d'être victime de la même manière).

En particulier, Son & Kim (2008) montrent que les bénéfices sociétaux de la plainte ont une influence directe uniquement sur les plaintes. Ce constat repose essentiellement sur les théories des lanceurs d'alerte (*whistleblowing*), indiquant que les dénonciations faites par des employés

⁷¹ Les justices perçue, distributive, procédurale et interactionnelle (Lind & Tyler, 1988; Rawls, 2004) sont respectivement le degré de justice perçu par un utilisateur dans sa relation avec un fournisseur, le degré perçu de bonne répartition des bénéfices et avantages entre l'utilisateur et le fournisseur, le degré de clarté, transparence et bon respect des procédures de contrôle de ses données personnelles, le degré d'honnêteté et de confiance perçus dans le traitement de ses données personnelles.

concernant de mauvaises pratiques managériales proviennent essentiellement d'une volonté de protéger d'autres salariés des mêmes mauvaises pratiques (Dozier & Miceli 1985).

Figure 12 : Réponses pour la protection de la vie privée (Son & Kim, 2008)



2.2. Retour critique sur les comportements de réponse face à une violation de la vie privée

2.2.1. Proposition d'une nouvelle classification des réponses à une violation de la vie privée

La taxonomie séminale de Son & Kim (2008) est une base fondatrice pour étudier les comportements de réponses face à une violation de données personnelles. Or depuis 2008 (année de publication de l'article de Son & Kim), les possibilités de réponses des consommateurs ont très largement évolué, notamment du fait des réglementations entrées en vigueur. De plus, la digitalisation de nos vies et économies s'est accentuée, rendant impossible dans certains cas de quitter des services (e.g., de missions publiques et/ou qui font appel à des sociétés privées, notamment dans le domaine de la santé⁷²). Malgré cela, la taxonomie de Son & Kim n'a, à notre connaissance, pas été significativement actualisée, du fait que très peu de recherches portent sur les réponses des consommateurs face à une violation de données personnelles.

Dans le cas d'une violation de leurs données personnelles, les consommateurs ont la possibilité, tout en restant loyaux, d'appliquer des mesures de sécurité, telles que l'authentification et le contrôle d'accès (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018) pour se protéger de futures violations de données. Ils peuvent également agir en refusant la divulgation de certaines informations ou en falsifiant leurs données (option de sortie indirecte) (Miltgen & Smith, 2019).

Les consommateurs peuvent choisir l'option *exit*, et supprimer ou arrêter d'utiliser le service en ligne ou le réseau social (option de sortie). Dans ce cas, les réglementations en vigueur (e.g., RGPD en Europe) leur permettent de demander une restitution et/ou un effacement de leurs données personnelles.

Les consommateurs peuvent se plaindre auprès d'un tiers spécialisé dans la protection des données personnelles (e.g., BBBonline, TRUSTe⁷³), des associations de défense des consommateurs, du médiateur européen (European Ombudsman), et de l'autorité de protection

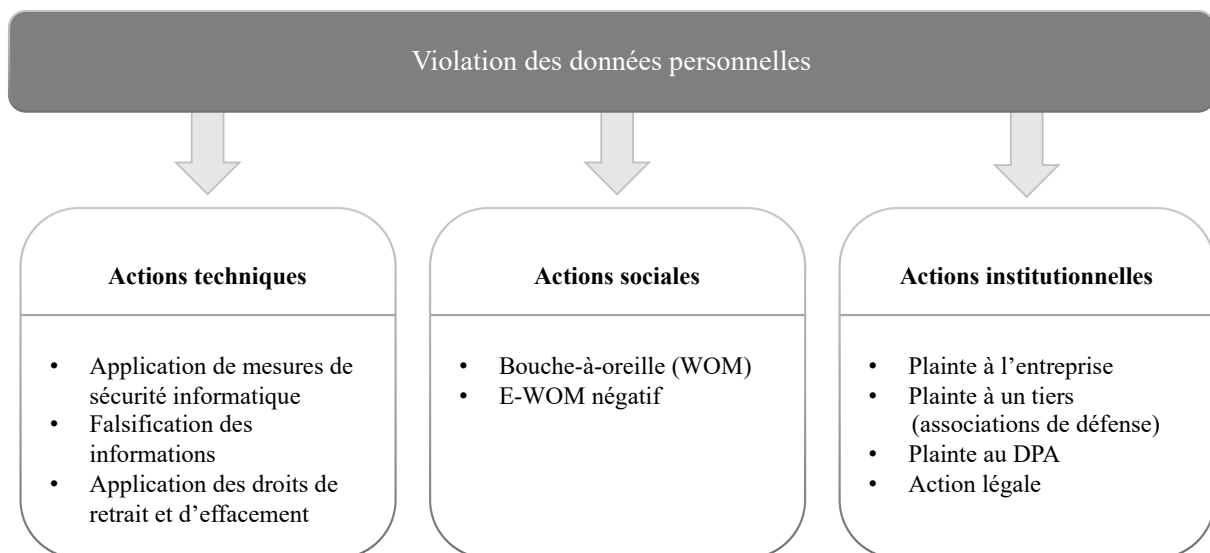
⁷² Exemple de Doctolib

⁷³ TRUSTe est un tiers de certification qui permet aux entreprises d'assurer à ses clients qu'elle a des pratiques de traitement de données personnelles conformes à la réglementation. Ainsi si une entreprise certifiée TRUSTe est à l'origine de la violation de données personnelles, alors l'utilisateur peut porter plainte à TRUSTe qui jouera le rôle de médiateur en vue de trouver une solution.

des données (ou DPA pour Data Protection Authority ; e.g., la CNIL en France). Ils peuvent mener des actions militantes indépendantes ou collectives (e.g., la Quadrature du Net), qui peuvent déboucher sur des actions de dénonciation. Ils ont la possibilité de mener des actions en justice (Mamonov & Benbunan-Fich, 2018; Romanosky et al., 2013), visant une compensation financière, notamment lorsque les violations de données personnelles sont clairement constatées.

Nous proposons donc un nouveau modèle ci-après : cf. Figure 13. Ce modèle, qui exclut les réponses « je ne fais rien » et « j’abandonne le service » est organisé autour de trois sections : actions techniques, actions sociales et actions institutionnelles.

Figure 13 : Réponses face à une violation de données personnelles



2.2.2. Antécédents au comportement de réponse

Plusieurs recherches ont identifié d'autres antécédents au comportement de réponse face à une violation de données personnelles : le stress et la violation perçus d'un contrat social (moral) entre l'entreprise et le consommateur (Labrecque, 2021), le sentiment de vulnérabilité, la menace d'activités frauduleuses (Kshetri, 2014).

Comme nous l'avons vu dans la littérature en CCB, beaucoup d'autres antécédents pourraient être étudiés : par exemple, rôle social, facteurs d'expérience et de capacité. L'importance de la vulnérabilité pourrait être approfondie. Abordons l'étude de ces antécédents avec vigilance.

D'une part, il n'est pas confirmé que le comportement de réponse à l'atteinte à la vie privée semble suivre un processus différent du comportement de plainte classique (Sheehan & Hoy, 1999). D'autre part, les stratégies d'adaptation dans le cas des atteintes à la vie privée utilisent de multiples facettes et sont complexes (Cho et al., 2020). Face à cette complexité, les antécédents pourraient être abordés par des typologies de profils en mobilisant les typologies de Singh (1990) (*passive, voicers, irates, activist*), de Westin (1967) (Sheehan & Hoy, 1999), ou d'autres typologies plus récentes portant sur la vie privée (Elueze & Quan-Haase, 2018; Koops et al., 2016; Miltgen, 2010).

Synthèse de la section sur les réponses des consommateurs insatisfaits

Les réponses des consommateurs insatisfaits sont des tentatives de clients cherchant à modifier une situation insatisfaisante, qui passent par des phases d'évaluation psychologique, de capacité sociétale, d'évaluation du cadre juridique et de stratégies de réponse. Ce processus est diachronique, évolutif, complexe. Une compréhension des réponses des consommateurs insatisfaits doit passer par une analyse à différents niveaux d'observation.

De plus, les réponses peuvent être absentes, privées ou publiques. Dans le cas d'une violation de leurs données personnelles, elles peuvent être techniques, sociales, institutionnelles. Et les réponses ont des antécédents tant psychologiques que sociétaux (e.g., self-efficacy et rôles sociaux).

Enfin, une violation de données personnelles est considérée comme la rupture d'un contrat social et de confiance qui lie une entreprise et ses clients : est-on alors réellement dans la situation d'un consommateur insatisfait ? s'agit-il simplement d'une attente non satisfaite ?

Section 3. Culture et valeurs culturelles

“Culture hides more than it reveals” (Hall, 1976)

*“Every person is a certain respect like all others,
like some others, and like no others”* (Kluckhohn et al., 1953)

Cette section est ambitieuse au regard de la myriade de définitions que revêt la culture, qui a été étudiée dans de nombreuses disciplines (e.g., anthropologie, sociologie, philosophie, psychologie). Nous avons dû faire des choix, qui n’ont pas toujours été faciles, pour nous concentrer sur les aspects de la culture importants pour notre sujet.

Nous exposons dans une première partie le concept de culture de manière générale, à travers son histoire et ses grandes acceptations. Nous expliquons notamment comment la culture est composée d’éléments explicites et implicites (dont les normes et les valeurs) et nous concentrons sur la notion de valeurs, que nous définissons. Puis dans une troisième partie, nous exposons les grandes théories des valeurs, que nous utilisons dans la suite de notre recherche. Nous détaillons les modèles d’Hofstede, de Schwartz et faisons un focus sur l’individualisme, dimension utilisée majoritairement dans les recherches en vie privée (cf. supra). Nous finissons avec un retour critique sur les différents modèles, concluant sur la nécessité d’adopter une approche multi-niveaux (macro, méso, micro) pour une étude des effets culturels.

1. Définition du concept de culture

L'objectif dans cette première partie est de poser les fondements historiques du concept de culture (1.1), de faire la distinction entre culture et contexte (1.2) et de présenter la culture selon ses différents aspects, des plus explicites comme le langage ou plus implicites comme les valeurs (1.3).

1.1. Développement historique du concept de culture

1.1.1. Culture et anthropologie à partir du XVIIIème siècle

Le terme culture apparaît au XVIIIème siècle : les philosophes des Lumières font la distinction entre nature et culture, signe distinctif de l'espèce humaine et « somme des savoirs accumulés et transmis par l'humanité, considérée comme totalité, au cours de son histoire » (Cuche, 2020, p.11). En 1798, la culture est définie dans le Dictionnaire de l'Académie comme « Du soin qu'on prend des arts et de l'esprit »⁷⁴. La notion de culture évolue au cours du XVIIIème siècle pour faire apparaître une « science de l'homme » (Diderot & Alembert, 1777), se distinguant des enseignements de l'Église. Le développement de la « science de l'homme » aboutira à la naissance de l'ethnologie (en 1787) et de l'anthropologie dont l'objectif commun est d'étudier, avec différents moyens et outils, l'être humain et les groupes humains dans toute la diversité de leurs us et coutumes. Edward Burnett Tylor, anthropologue britannique, définit pour la première fois le concept de culture en 1871 :

« Culture ou civilisation, pris dans son sens ethnologique le plus étendu, est ce tout complexe qui comprend la connaissance, les croyances, l'art, la morale, le droit, les coutumes et les autres capacités ou habitudes acquises par l'homme en tant que membre de la société » (Tylor, 1871, p.1).

Pour Tylor, la culture est collective, acquise et universelle. L'étude de la culture se veut descriptive et non normative, pour éviter tout dogmatisme et stéréotype : « Héritier des Lumières, il adhère également à la conception universaliste de la culture des philosophes du

⁷⁴ <https://www.dictionnaire-academie.fr/article/A5C3115>

XVIIIème siècle » (Cuche, 2020, p.19). La difficulté est alors d'expliquer les différences et les évolutions entre nations ou groupes sociaux tout en pensant l'universalité de la culture.

Bien sûr, l'universalité de la culture fait l'objet de très nombreux débats, notamment entre d'un côté penseurs français, attachés à l'idée d'unité collective (comme en témoigne la déclaration d'Ernest Renan en 1882: « Avant la culture française, la culture allemande, la culture italienne, il y a la culture humaine » (Renan, 1882)); et d'un autre côté les penseurs allemands, attachés aux différences et diversités, et qui distinguent *culture* et *civilisation*. Ces débats engendrent des évolutions dans la compréhension du concept de *Culture*. À titre d'exemple, la définition de *Culture* en 1935 toujours dans le Dictionnaire de l'Académie⁷⁵ est la suivante : Culture « se dit figurément de l'application qu'on met à perfectionner les sciences, les arts, à développer les facultés intellectuelles (...). Culture générale : ensemble de connaissances générales sur la littérature, l'histoire, la philosophie, les sciences et les arts, que doivent posséder, au sortir de l'adolescence, tous ceux qui forment l'élite de la nation. Par extension de ces deux derniers sens, Culture est quelquefois maintenant synonyme de Civilisation. *Culture gréco-latine. Propager la culture française à l'étranger* ».

Derrière le terme culture se cachent les idées de *race*, de *primitifs* ou de *sauvages*, de *hiérarchie de civilisations*. Nous ne détaillerons pas la diversité et l'objet de ces débats, qui ne font pas l'objet de notre recherche. De cet héritage, nous retiendrons l'universalité de la culture, qui guidera nos choix conceptuels dans la suite de cette dissertation.

Dans la lignée de Tylor, l'anthropologue allemand Franz Boas (1858-1942), à travers ses recherches sur les Indiens d'Amérique du Nord, soutient l'idée qu'il n'existe pas de différence naturelle, biologique ou raciale entre les hommes, mais uniquement culturelle et acquise : chaque culture se vaut et mérite respect, et il n'existe pas de hiérarchie entre les cultures.

⁷⁵ <https://www.dictionnaire-academie.fr/article/A8C3658>

1.1.2. Culture et fait social à partir de Durkheim

Le contemporain de Franz Boas, Emile Durkheim (1858-1917), soutient la même idée :

« Le développement humain doit être figuré, non sous la forme d'une ligne où les sociétés viendraient se disposer les unes derrière les autres comme si les plus avancées n'étaient que la suite et la continuation des plus rudimentaires, mais comme un arbre aux rameaux multiples et divergents. Rien ne nous dit que la civilisation de demain ne sera que le prolongement de celle qui passe aujourd'hui pour la plus élevée ; peut-être au contraire aura-t-elle pour agents des peuples que nous jugeons inférieurs comme la Chine par exemple, et qui lui imprimeront une direction nouvelle et inattendue » (Durkheim, L'Année sociologique, tome XII, 1913, p.60-61).

De plus, l'œuvre de Durkheim met en avant quatre idées importantes : (i) tout phénomène social a une dimension symbolique donc culturelle, (ii) une civilisation est un ensemble de phénomènes sociaux qui s'étend géographiquement et temporellement sur des aires plus larges qu'une nation (ainsi une culture ne peut pas être que nationale), (iii) il existe une « conscience collective », faite d'idéaux, de valeurs et de symboles à tous les individus de la société, (iv) cette « conscience collective » s'impose à l'individu.

De cela, nous retenons la définition de la culture que nous adoptons : la culture est une conscience collective faite de valeurs universelles et de symboles, partagée par un groupe social particulier, et qui dépasse les frontières nationales.

Par la suite, l'objectif des anthropologues, des ethnologues puis des sociologues est de comprendre comment l'individu est relié à sa culture, comment la culture se distingue du contexte dans lequel elle agit et comment les éléments implicites de la culture agissent. Nous allons donc préciser la différence entre culture et contexte, puis la différence entre éléments explicites et implicites de la culture.

1.2. Distinction entre culture et contexte

Nous nous interrogeons souvent sur la différence entre culture et contexte : Est-ce qu'un phénomène observé est culturel ou contextuel ? Est-ce que répondre face à une violation de ses données personnelles est lié à la culture (i.e., une conscience collective constituée de valeurs et de symboles) ou au contexte (e.g., maturité digitale, connaissance de la loi) ?

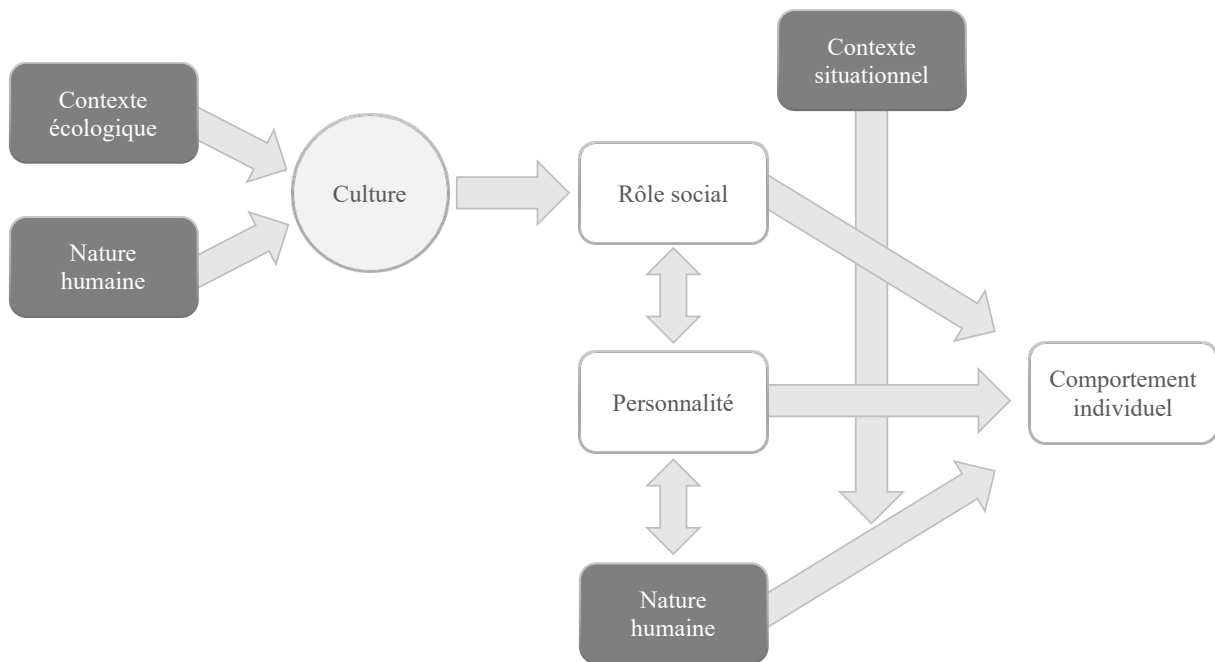
Pour comprendre la distinction entre les deux, nous adoptons la vision de Matsumoto. Matsumoto (2007) distingue trois facteurs contextuels (cf. Figure 14) :

- Le contexte écologique (climat, géographie, densité de population),
- La nature humaine (besoins universels, motivations sociales, processus psychologiques),
- Les facteurs situationnels, i.e., la pression du temps, les incitations externes, les récompenses et punitions, qui influencent la relation valeurs-comportements, avec des niveaux de sensibilité différents selon notre déterminabilité sociale (Maio et al., 2006).

En d'autres termes, ces facteurs contextuels sont variables (peuvent changer) alors que la culture en tant que conscience collective est stable. Le contexte est constitué de tout ce qui peut influencer un processus déjà connu (Denis & Le Ny, 1993).

Ces facteurs contextuels agissent en entrée et en sortie du processus qui aboutit aux comportements individuels. Les comportements individuels résultent de l'interaction entre nature humaine (processus psychologiques universels et fondamentaux de la nature humaine), personnalité (identités individuelles) et rôle social. Le rôle social intègre les éléments culturels qui se retrouveront dans le comportement individuel. Le rôle social est le résultat de la lecture du contexte écologique et de la nature, passé par le filtre de lecture de la culture, i.e., interprété par un système de pensée partagé par un groupe d'individus. Ce système de pensée, composé d'éléments et de valeurs (que nous allons préciser par la suite) va agir comme un filtre d'interprétation des éléments biologiques (nature humaine) et environnementaux (écologiques) (Chiu & Hong, in Kruglanski & Higgins, 2007). Le rôle social qui en résulte est culturellement dépendant.

Figure 14 : Influence de facteurs contextuels sur le comportement individuel (Matsumoto, 2007)

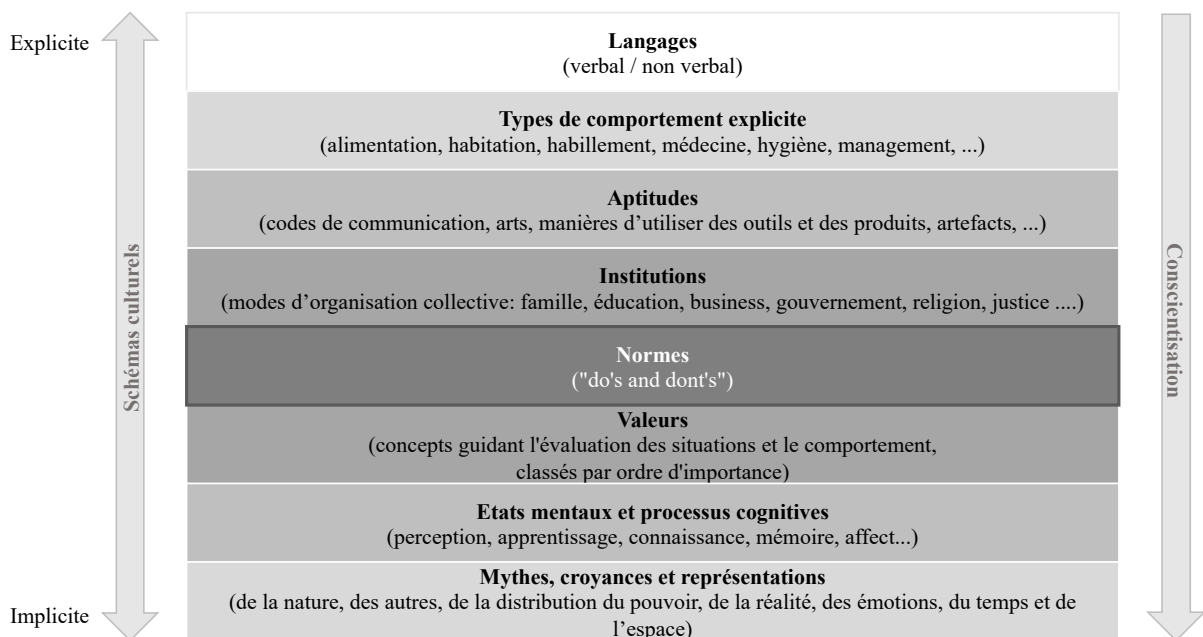


Cette différence entre culture et contexte est importante pour notre recherche. En effet, comme nous l'avons montré dans la section 1 de ce chapitre 2, la vie privée est considérée par certains chercheurs comme un construit contextuel et situationnel (Altman, 1975, Nissenbaum, 2004), amenant à des reconceptualisations de la préoccupation pour la protection de la vie privée selon les contextes d'observation (cf. Tableau 17). Or, nous pensons qu'une reconceptualisation doit pouvoir être stabilisée : pour cela, il nous semble nécessaire de mieux distinguer normes culturelles et valeurs stables, constitutives de la préoccupation pour la protection de la vie privée, des phénomènes contextuels changeants. **Nous proposons d'interroger cette différence entre contexte (notamment le contexte des violations de données personnelles), et justifiant des reconceptualisations multiples, et culture (plus stable) dans le chapitre 7 dédié à la discussion de nos résultats de recherche.**

1.3. Distinction entre niveaux explicites et implicites de la culture

Par ailleurs, la culture est composée d'éléments explicites et implicites, souvent représentés sous forme d'iceberg (avec une partie émergée et une partie immergée) : la culture émergée est celle de la culture visible, alors que la culture immergée est celle de la culture qui ne se voit pas (i.e., les normes, valeurs, processus cognitifs et représentations). Dans la Figure 15 ci-dessous, la partie émergée est la partie supérieure du schéma, la partie immergée est la partie inférieure.

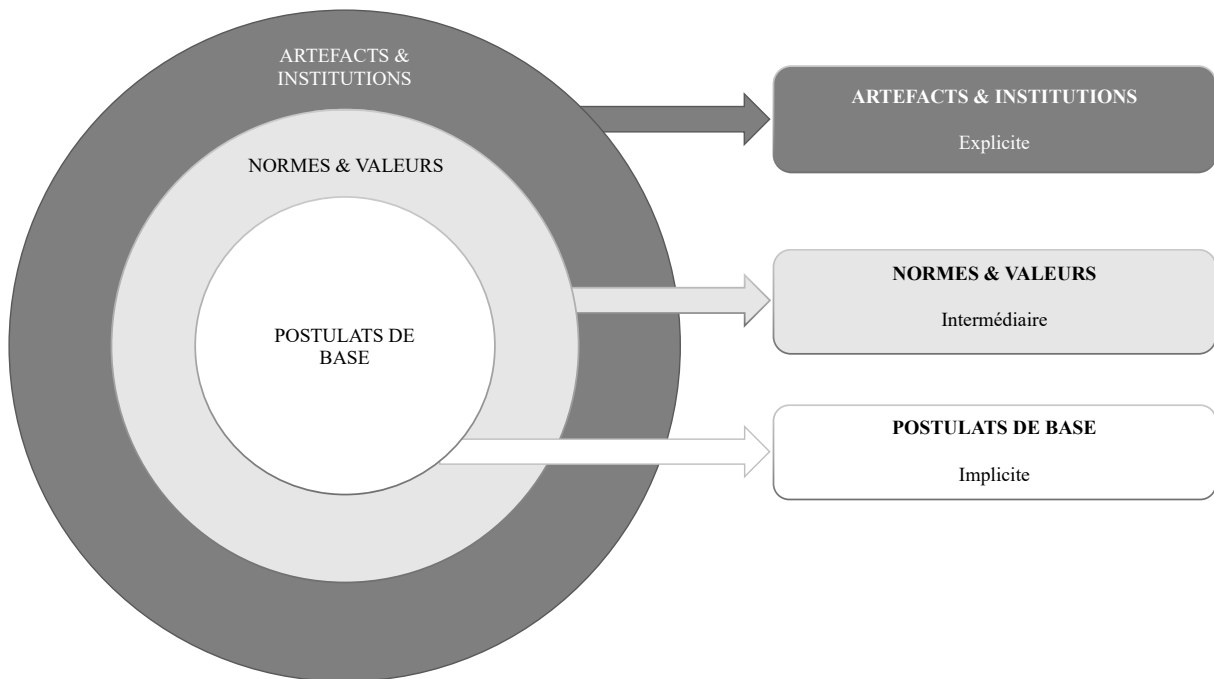
Figure 15 : Différents niveaux de culture (Prime & Usunier, 2012)



Cette représentation de la culture montre la multiplicité des aspects qui peuvent être pris en considération pour observer des effets culturels. Notamment les processus cognitifs (e.g., Hong et al. (2000) et les perceptions de temps et d'espace (Hall, 1976) ont beaucoup attiré notre attention au cours de notre réflexion sur ce travail doctoral. Ces points nécessitent une analyse approfondie qui n'a pas sa place dans notre recherche : nous avons écarté ces aspects de la culture pour nous concentrer sur les valeurs.

La culture peut aussi être représentée en trois blocs, tels que des strates superposées (Schein, 1984; Trompenaars & Hampden-Turner, 1998) ou un « Oignon » (Hofstede et al., 2010), allant du niveau le plus implicite au niveau le plus explicite (cf. Figure 16). Les institutions, porteuses des normes et des valeurs, peuvent être incluses ou non au sein des artefacts (Hoult, 1969).

Figure 16 : Trois blocs composant la culture (adapté de Schein et al. (2015), Trompenaars (1996) et Hoult (1969))



Quelles différences entre normes, valeurs et postulats de base ? :

- Les normes sociales sont des règles de conduite (explicites ou implicites) qui orientent le comportement des individus conformément aux valeurs de la société. Par exemple, il n'est pas convenable dans une société occidentale de se promener dans la rue en pyjama.
- Une valeur est un principe moral, un idéal auquel les membres d'une société adhèrent et qui se manifestent concrètement dans leurs manières de penser et d'agir. Par exemple, il n'est pas accepté en France que la chaîne de restaurant Mac Donald's congédie un salarié parce qu'il a offert des hamburgers à un sans-abri. Les normes peuvent entrer en contradiction avec les valeurs et influencer les intentions comportementales (Ajzen & Fishbein, 1975).

- Enfin, les postulats collectifs de base, sont les éléments les plus implicites de la culture, auparavant des valeurs et qui ne sont plus conscientisées, devenant une « programmation de l'esprit » (Hofstede et al., 2010).

Notre recherche s'intéresse aux valeurs, définies comme principe moral plus ou moins conscientisées, qui agissent sur les manières de penser et d'agir. Nous allons préciser le concept de valeurs dans le paragraphe suivant.

*

Nous venons de présenter les fondements historiques de la culture, apparue au XVIIIème siècle avec les philosophes des Lumières et définie comme une « science de l'homme », conceptualisée pour la première fois en 1871 par l'anthropologue Tylor, et repris ensuite par les sociologues, notamment Durkheim : la culture est définie comme une conscience collective faite de valeurs universelles et de symboles, partagée par un groupe social particulier, et qui dépassent les frontières nationales. Nous spécifions dans le paragraphe suivant la notion de valeurs culturelles.

2. Définition et compréhension des valeurs culturelles

« Les valeurs sont des conceptions centrales du désirable dans chaque individu et dans la société. Elles servent de standards ou de critères pour guider non seulement l'action mais aussi le jugement, le choix, l'attitude, l'évaluation, l'argumentation, l'exhortation, la rationalisation, et, on pourrait ajouter, l'attribution de la causalité » (Rokeach, 1979, p.2).

Cette partie est consacrée à la compréhension des valeurs culturelles, que nous définissons (2.1) avant d'exposer les processus de développement et de socialisation (2.2).

2.1. Définition des valeurs culturelles

Un système de valeurs est un ensemble de règles apprises permettant à une personne de choisir entre des alternatives, à résoudre des conflits et à prendre des décisions (Rokeach, 1973), basé sur le principe qu'un mode de conduite ou un état final d'existence est préférable à un autre. Ces valeurs sont universelles : tous les hommes dans le monde possèdent les mêmes valeurs à des degrés différents, il existe une « organisation universelle des motivations humaines » (Schwartz, 2006), et seule change la structure des valeurs entre elles au sein de groupes de cultures différentes. Les valeurs sont reliées entre elles, et sont organisées sous forme de système : elles vont donc soit se compléter, soit s'opposer, tout en évoluant ensemble (permettant une stabilité individuelle et sociale). Ces valeurs sont transmises par les institutions, par les processus de socialisation, et forment un kit symbolique de traduction de l'environnement. En petit nombre, les valeurs sont intériorisées et deviennent cachées, subtiles (Hall, 1959), implicites, un référentiel de sens, un ensemble d'idéaux repères qui structurent l'ordre éthique (Bourqia, 2006, 2010) et relèvent surtout de la psychologie (Oyserman, 2012), mais également hyper-normes servant de fondement aux cadres institutionnels. Ainsi, les valeurs sont des croyances d'ordre cognitif, affectif, et comportemental. Enfin, elles sont stables dans le temps (e.g., un faible niveau de confiance dans les institutions perdurera des grands-parents aux petits-enfants ; Uslaner, 2008), mais évolutives, au gré des années et de l'âge.

Nous retenons trois caractéristiques principales des valeurs : les valeurs sont avant tout culturelles (donc universelles), implicites (donc abstraites) et permettent d'établir un cadre éthique (qui peut évoluer).

Nous souhaitons insister sur le fait que toute valeur a un contenu culturel (Rokeach, 2008) :

- Schwartz (1994) identifie 7 dimensions culturelles (e.g., l'autonomie et la place dans le groupe, le maintien de l'ordre social, la relation à l'environnement social et naturel), mobilisées dans le cadre de conflits sociétaux ou questions majeures auxquels toute culture ou groupe doit répondre (Chataigné, 2014) ;
- Le terme « culturel » nous semble employé essentiellement pour identifier des différences nationales, qu'elles soient multiculturelles, transculturelles ou interculturelles⁷⁶. Or la culture ne peut être limitée à des frontières nationales (comme Durkheim l'a indiqué), ce qui est d'autant plus vrai dans un monde est de plus en plus déterritorialisé, où les populations voyagent et communiquent entre elles, entraîne une contamination culturelle et un pluralisme culturel (Craig & Douglas, 2006). De plus il peut exister plus de différences entre des individus du même pays qu'entre pays (Fischer et al., 2010; Fischer & Schwartz, 2011) ;
- En outre, la culture doit être comprise comme un vecteur de sens permettant à un groupe social de disposer de filtres communs de traduction de l'environnement (Matsumoto, 2007) : un élément est dit culturel s'il possède un sens (une symbolique) pour les agents qui les assument.

Ainsi, tout fait social est symbolique donc culturel (Mauss & Durkheim, 1913) et les valeurs ont toujours un contenu culturel (Rokeach, 2008).

En conclusion, dans notre thèse, nous nous reposons sur la définition de la culture suivante :

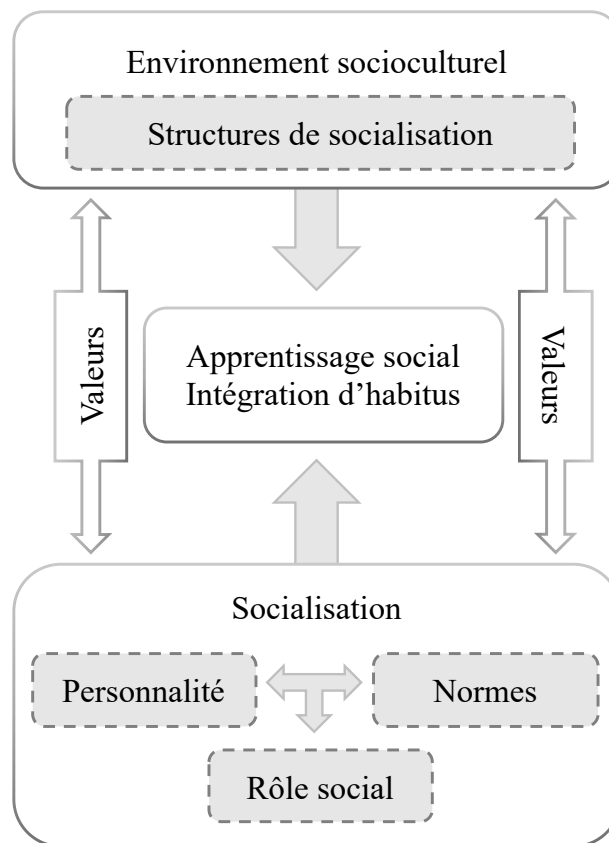
La culture est un ensemble de valeurs universelles, implicites, des symboles qui donnent du sens à l'action et à la décision.

⁷⁶ Une recherche multiculturelle comparent des sociétés avec différentes cultures isolées ; une recherche cross-culturelles étudie une société où une culture est la norme et les autres se comparent à la norme ; une recherche interculturelle étudie des sociétés ayant une compréhension et un respect profond entre les cultures (Schriefer, 2016; Gudykunst, 2003).

2.2. Valeurs et processus de socialisation

Par ailleurs, les valeurs tirent leurs forces de leurs formes de transmission et d'expression dans des cadres de socialisation et d'apprentissage social, de facto culturels (cf. Figure 17). Les valeurs sont le résultat à la fois de l'héritage culturel et des expériences personnelles (Rokeach, 1973), enseignées pendant l'enfance (avant 10 ans). Les valeurs sont transmises par des institutions (famille, école et structures éducatives, entreprises, associations), des processus de socialisation ou apprentissage social (Bandura, 1977; Bourdieu, 1979) qui consistent à apprendre en observant des modèles, imiter et reproduire efficacement certains comportements sociaux, ou encore des interactions individuelles (Sapir, 1921).

Figure 17 : Rôle des valeurs dans les processus de socialisation (Ladwein, 2003)



Par conséquent, les valeurs peuvent être spécifiques à un pays, à un groupe social (e.g., une génération, une minorité sociale ou « ethnique ») mais également à chacun. En effet, chaque individu a sa propre façon d'intérioriser et de vivre sa culture (Kardiner, 1939) et de faire évoluer la culture à travers les échanges et les interactions individuelles. Ces valeurs vont ensuite structurer un style de vie (Kahle & Valette-Florence, 2012; Valette-Florence, 1986).

Les valeurs deviennent implicites, des construits centraux (Rokeach, 1973; Schwartz, 1992), très peu controversées car universelles (les questionnements portant généralement sur les conflits de valeurs que sur les valeurs elles-mêmes). Elles peuvent ainsi être considérées comme des truismes culturels car partagés au sein d'un groupe : « *Les truismes culturels sont des croyances qui sont si largement partagées dans le milieu social de la personne qu'elle ne les aurait jamais entendu être attaqués, et par conséquent, pour lesquels elle douterait qu'une attaque soit possible* » (McGuire, 1964, p.201).

Devenues implicites et abstraites, les valeurs structurent un ordre moral, une éthique. Ces valeurs vont servir de base à la constitution d'un cadre éthique universel (e.g., les Droits de l'Homme) et d'un cadre réglementaire et législatif propre à chaque pays (e.g., Constitution d'un pays), à chaque culture ou à chaque groupe social (e.g., Déclaration d'indépendance du cyberspace de John Perry Barlow⁷⁷). Pour exemple, le traité de Lisbonne (2007) définit des valeurs spécifiques à l'Europe (European values of Treaty of Lisbon) qui sont : la dignité humaine, la liberté (notamment de circulation dans l'Union, la démocratie (notamment représentative) et l'égalité (de tous devant la loi).

Pour revenir au sujet de notre recherche, des normes culturelles (telles que l'individualisme ou la distance hiérarchique, que nous allons préciser dans la partie suivante) affectent la conception et la mise en œuvre des réglementations sur la protection de la vie privée (Martin & Palmatier, 2020).

Par conséquent, la culture, définie comme un ensemble de valeurs universelles, implicites, des symboles qui donnent du sens à l'action et à la décision, influence le souci de contrôle des données personnelles à plusieurs niveaux : dans la façon d'appréhender ses décisions (donc par un truchement psychologique) ou dans la façon de comprendre les réglementations (donc de façon plus institutionnelle ou globale). Ces valeurs sont également transmises socialement : notre recherche vise notamment à comprendre l'influence de la culture sur les réponses aux violations de données avec un regard sociologique.

⁷⁷ Déclaration d'indépendance du cyberspace de John Perry Barlow, publiée le 9 février 1996 sur le site web de l'Electronic Frontier Foundation, accessible à : <https://www EFF.org/fr/cyberspace-independence>

*

Les valeurs sont universelles, stables dans le temps, acquises par des processus de socialisation, propres à un pays, à un groupe social et spécifique à chaque individu. Devenues implicites et abstraites, elles forment un kit de traduction de l'environnement et le socle d'un cadre éthique sur lequel reposent les règles et les lois spécifiques à chaque groupe social. Implicitement, elles affectent la conception des réglementations sur la protection de la vie privée. Elles font l'objet de conceptualisations, que nous précisons maintenant.

3. Théories et structures de modèles de valeurs culturelles

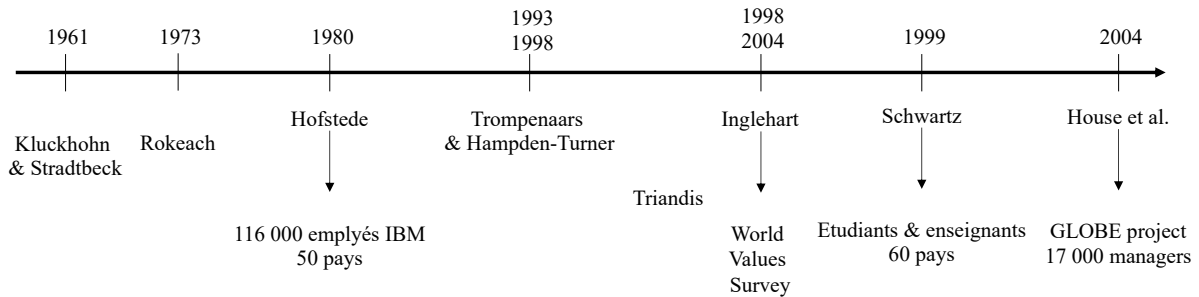
Les valeurs culturelles ont fait l'objet de nombreuses conceptualisations. Dans cette partie, nous présenterons les contributions majeures à la théorie des dimensions culturelles (3.1), que nous détaillons ensuite. Nous commençons les dimensions de la culture nationale d'Hofstede (3.2), nous faisons un focus sur la dimension d'individualisme précisée par Triandis (3.3), nous présentons les travaux de Schwartz (3.4) et nous concluons avec un retour critique sur ces différents modèles (3.5).

3.1. Contributions majeures à la théorie des dimensions culturelles

Après avoir abordé la culture à travers une description ethnographique (Soares et al., 2007), les anthropologues et les chercheurs en sciences sociales se sont attachés depuis 60 ans à représenter et conceptualiser les éléments subjectifs de la culture, à travers des valeurs et dimensions culturelles (une dimension étant un type motivationnel regroupant des valeurs simples).

Après les textes fondateurs entre autres de Spranger (1928), Maslow (1954) ou Kluckhohn & Strodtbeck (1961), Rokeach (1973) a défini un ensemble de 36 valeurs. Par la suite, Hofstede (depuis 1980) a lancé la plus importante étude basée sur 116.000 employés d'IBM dans 50 pays et fournissant 6 dimensions de la culture nationale (e.g., l'individualisme). Trompenaars & Hampden-Turner (1998) proposent un autre ensemble de 7 dimensions de la culture, basé sur 46.000 questionnaires dans 40 pays. Triandis (1993) différencie l'individualisme et le collectivisme verticaux et horizontaux. Inglehart (e.g., Inglehart & Carballo, 1997; Inglehart & Welzel, 2010) développe le World Values Survey, et distingue valeurs « matérialistes » et « post-matérialistes » (besoins fondamentaux vs. complexes). Schwartz (1999, 2006) étudie la relation entre valeurs individuelles et cultures nationales. House et al. (2004), avec le projet GLOBE qui comprend 17.000 managers, s'intéresse à la différence entre les valeurs et pratiques culturelles (Moalla, 2016). Cette chronologie des contributions à la théorie des dimensions culturelles est présentée dans la Figure 18 ci-après.

Figure 18 : Chronologie des contributions majeures à la théorie des dimensions culturelles



Parmi ces recherches, nous présentons en premier les dimensions de la culture nationale d'Hofstede, qui apportent un cadre culturel national fondamental. La dimension d'individualisme d'Hofstede est une dimension phrase, qui est majoritairement utilisée dans les recherches portant sur l'influence de la culture sur la préoccupation pour la protection des données personnelles : nous détaillons alors la dimension d'individualisme et nous exposons à cette occasion les travaux de Triandis (analyse multidimensionnelle de l'individualisme et du collectivisme). Puis nous détaillons les valeurs de Schwartz (qui reprennent les valeurs de Rokeach, qui elles-mêmes reprennent les valeurs de Kluckhohn).

3.2. Théorie des dimensions de la culture nationale d'Hofstede

Le modèle d'Hofstede (1980, 2001, 2010) provient d'un vaste projet de recherche conduit auprès de salariés de filiales d'IBM dans plus de 50 pays. Le modèle d'Hofstede a été présenté de façon détaillée en pages 68 et 69. Nous rappelons uniquement pour mémoire les 6 dimensions : distance hiérarchique, individualisme, masculinité, contrôle de l'incertitude, orientation à long terme et indulgence.

3.3. Focus sur la dimension d'individualisme

Parmi ces dimensions, l'individualisme (vs. collectivisme) est plus étudié que les autres, identifié comme un « syndrome culturel » (Triandis, 1993) et la « structure profonde » des différences culturelles, à partir de laquelle toutes les autres différences ont évolué (Greenfield, 2000). Bien que l'importance de l'individualisme - collectivisme puisse être vraie, elle doit être nuancée, notamment en raison de la grande variabilité individuelle au sein d'un seul pays, notamment aux États-Unis (Oyserman et al., 2002). De plus, les recherches sur la préoccupation pour la protection de la vie privée (Miltgen & Peyrat-Guillard, 2014) mobilisent essentiellement les dimensions d'Hofstede, et parmi elles, l'individualisme-collectivisme. Cependant, certaines recherches relèvent des résultats contradictoires. Afin de clarifier notre recherche, il semble nécessaire de préciser certains fondements historiques, idéologiques, économiques et culturels de la dimension individualisme-collectivisme ».

L'individualisme est défini comme une « doctrine qui fait de l'individu le fondement de la société et des valeurs morales »⁷⁸ et « favorisant la liberté d'action des individus au-delà d'un contrôle collectif ou étatique » (Oxford Dictionary), alors que le collectivisme repose sur un principe politique de propriété de la terre et des moyens de production par le peuple ou l'État. Ces définitions rendent compte du contenu politique et idéologique de la dimension d'individualisme-collectivisme. L'individualisme prend son origine avec les philosophes des Lumières. L'indépendance intellectuelle, l'autonomie de choix et d'expression est la condition de la bonne représentation du peuple et de la volonté générale (J.J. Rousseau, Déclaration universelle des droits de l'homme et du citoyen, Article 6, 1789). À la même période, Adam Smith soutient que l'individu ne peut pas s'enrichir et améliorer son bien-être sans être individualiste, idée renforcée par les mouvements protestants valorisant l'autonomie et la recherche d'intérêts personnels. Ultérieurement, Freud puis Jung identifient le processus d'individuation (par lequel un individu se détache et se dissocie du groupe), comme central process au développement humain. **Ainsi, l'individualisme est le symbole des démocraties libérales, également associé à une croissance économique forte (Inglehart, 2018), qui implique de ce fait bien-être, sécurité, stabilité (vs. risque et incertitude), mais aussi mouvements de population, mixité et hétérogénéité sociale et culturelle, et par conséquent violences sociales.**

⁷⁸ <https://www.larousse.fr/dictionnaires/francais/individualisme/>

Ceci amène certaines sociétés en voie d'ouverture internationale et de développement économique à refuser une vision individualiste de leur société. À titre d'exemple, le roi Hassan II du Maroc avait interdit les maisons de retraite, citant (s.d.) : « Le jour où l'on ouvrira la première maison de retraite au Maroc, notre société sera en voie de disparition. »

Les sociétés passent d'un stade de *Gemeinschaft* (communauté) à *Gesellschaft* (société et individualisme) (Tonnies, 1887). Les principes de solidarité entre individus ne sont plus mécaniques, basés sur un partage de ressources avec un proche similaire, mais organiques, basés sur échange de ressources avec un autre différent (Durkheim, 1909). Cette différence entre individus peut varier d'une forte équivalence à une forte différence entre soi et les autres (respectivement structures horizontale vs. verticale). Ceci amène Triandis (Triandis, 1996) à distinguer 4 types de groupes sociaux (cf. Tableau 20), selon le rapport aux autres et l'acceptation de la distance hiérarchique.

Tableau 20 : Individualisme et collectivisme vertical et horizontal de Triandis (1996)

	Collectivisme	Individualisme
Vertical	Différence soi-autres Partage des ressources Structure hiérarchique Faible liberté Faible égalité <i>Ex. Inde, China</i>	Différence soi-autres Échange des ressources Structure hiérarchique Forte liberté Faible égalité <i>Ex. USA, France</i>
Horizontal	Équivalence soi-autres Partage des ressources Structure égalitaire Faible liberté Forte égalité <i>Ex. Israël (situation rare)</i>	Équivalence soi-autres Échange des ressources Structure égalitaire Forte liberté Forte égalité <i>Ex. Australie, Norvège</i>

Le rapport à l'autre étant différent, les normes sont plus importantes dans les sociétés collectivistes que les attitudes, pour prédire les comportements (Triandis, 1993; Fishbein & Ajzen, 1980). De plus, l'individualisme est corrélé à la justice sociale et à la paix dans le monde alors que le collectivisme est corrélé à la maîtrise sociale et l'harmonie avec la hiérarchie et l'organisation sociale (Triandis, 1993).

En conclusion, l'individualisme et le collectivisme, « syndromes culturels », doivent être considérés comme des « worldviews », i.e., des concepts macro dont l'expression va beaucoup dépendre du contexte dans lequel l'action se situe (Oyserman, 2012), et qui doivent être nuancés par l'ensemble des concepts qu'ils intègrent : sécurité, égalité sociale, croissance, risques, confiance (Westjohn et al., 2022) en apportant par exemple des regards historiques, anthropologiques ou économiques. En particulier, notre recherche, qui remet en question l'importance de l'individualisme dans la compréhension du souci de contrôle de ses données personnelles, doit interroger les dimensions de second degré et les valeurs qui constituent l'individualisme.

3.4. Théorie des valeurs de Schwartz

3.4.1. Héritage des valeurs terminales et instrumentales de Rokeach

La théorie des valeurs de Schwartz reprend les travaux de Rokeach (1973), qui définissent un ensemble de 36 valeurs terminales (i.e., des buts que l'individu poursuit dans sa vie pour lui-même ou pour son groupe social ; e.g., l'égalité entre individus ou la reconnaissance sociale) et des valeurs instrumentales (i.e., des manières d'être ou de se comporter qui permettent d'atteindre les valeurs terminales ; e.g., être courageux, être obéissant). Voici dans le Tableau 21 ci-dessous des exemples de valeurs terminales et instrumentales.

Tableau 21 : Exemples de valeurs terminales et instrumentales (Rokeach, 1973)

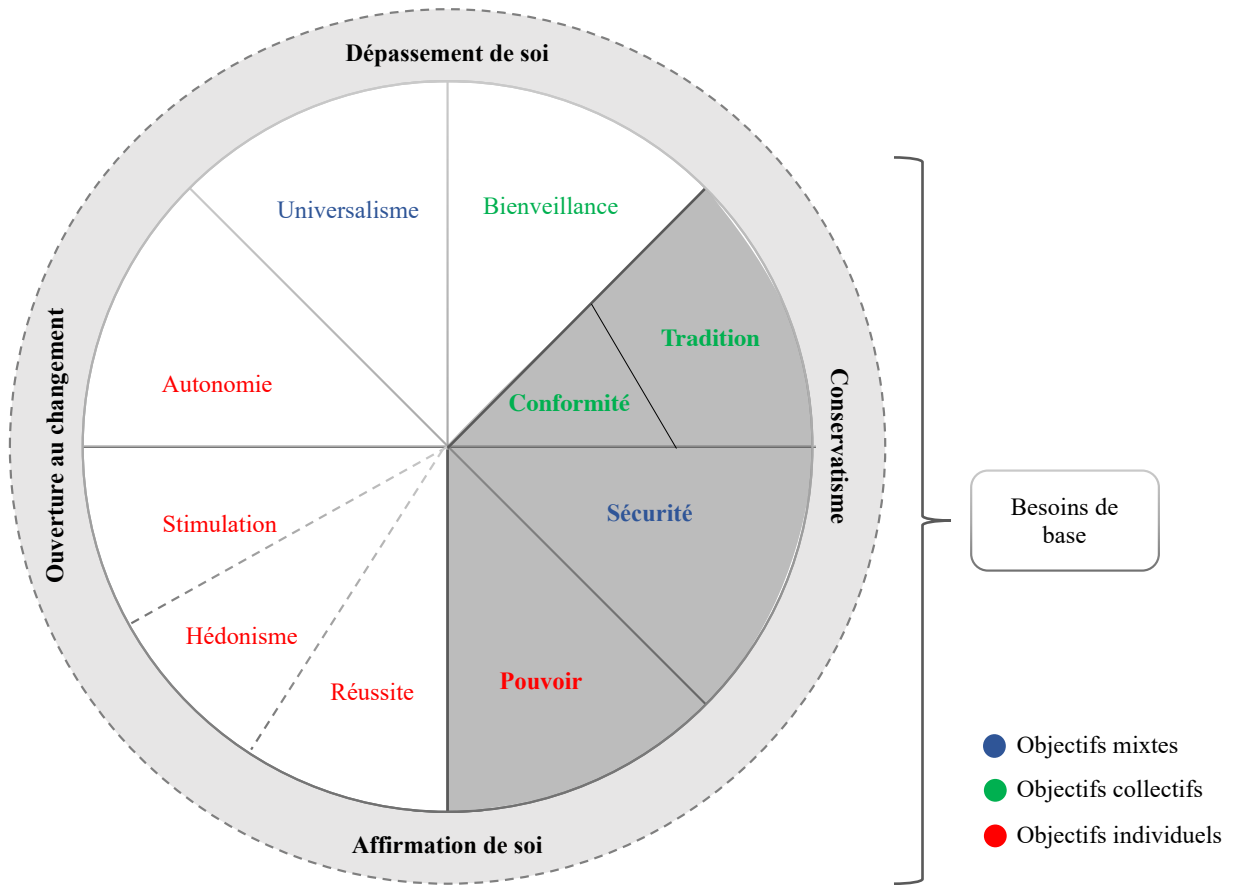
Valeurs terminales	Valeurs instrumentales
Une vie aisée (une vie prospère)	Ambitieux (travailleur, qui désire réussir)
La liberté (indépendance, libre choix)	Serviable (qui œuvre pour le bien des autres)
La sagesse (une compréhension réfléchie de la vie)	Maître de soi (mesuré, autodiscipliné)
La sécurité nationale (protection contre une attaque)	Intellectuel (intelligent / réfléchi)

Schwartz (1994) abandonne l'idée de valeurs terminales et instrumentales et les regroupe en un seul « but ». Il considère en effet que si pour des objectifs à atteindre à court terme, il est possible de distinguer fins et moyens, cette distinction n'est plus possible pour des objectifs lointains donc plus abstraits (Boudon & Bourricaud, 1982). Nous gardons cependant l'idée de Rokeach dans l'analyse empirique actuellement en cours pour notre chapitre 5 (essai 2 niveau méso).

3.4.2. Valeurs de Schwartz : universelles et reliées entre elles

Deux idées marquent les travaux de Schwartz. D'une part, les valeurs sont universelles : partagées par toutes les cultures dans le monde, les valeurs sont des objectifs souhaitables pour la survie et le développement du groupe, liant le groupe, aidant la communication au sein du groupe, coordonnant les actions du groupe. D'autre part, les valeurs sont liées les unes aux autres et peuvent être placées sur un disque, structure circulaire, en fonction de leur degré de proximité : cf. Figure 19 ci-après.

Figure 19 : Système initial de valeurs de Schwartz



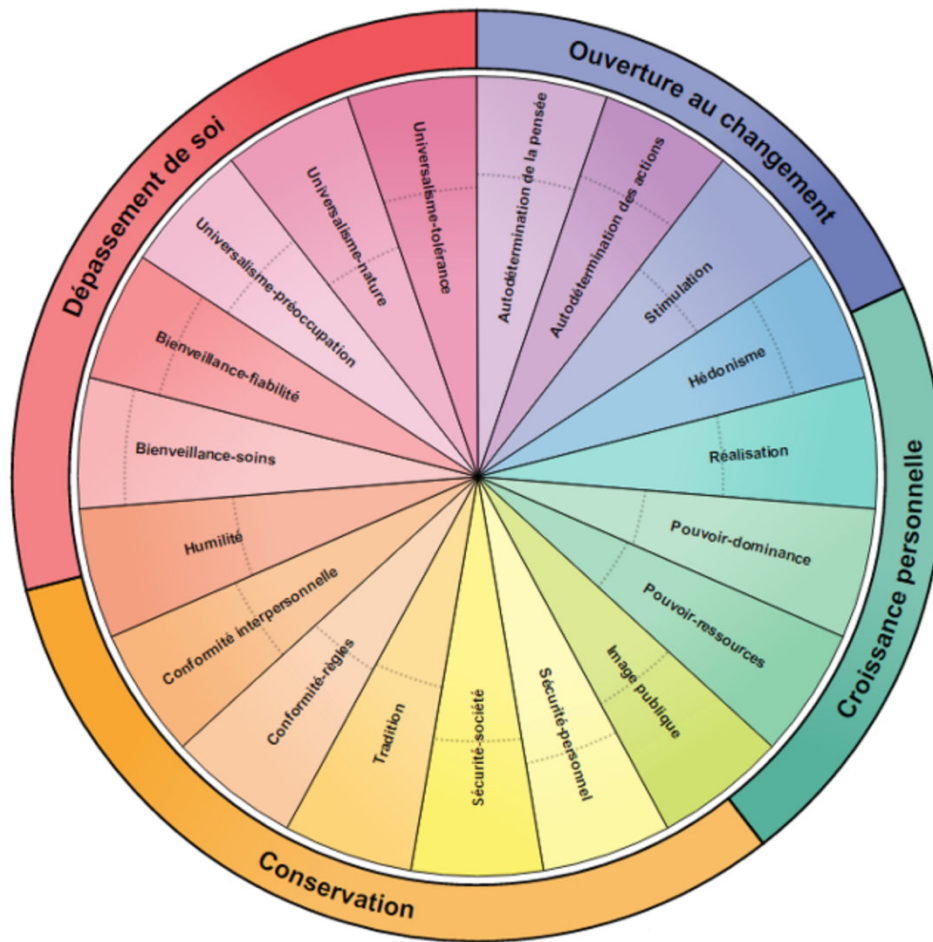
Réalisé à partir de la structure « Circumplex » du système des valeurs Schwartz (1992), la distinction intérêts individuels et intérêts collectifs (Schwartz, 1992) et l'analyse des valeurs de croissance ou de carence (Bilsky & Schwartz, 1994).

Le modèle initial comprend 10 valeurs universelles ou types motivationnels (Schwartz, 1992) (cf. Tableau 22). Les 10 valeurs sont placées le long de deux axes, illustrant les relations entre elles : axe « affirmation de soi vs. dépassement de soi », et axe « continuité vs. changement ». La spiritualité sera ensuite ajoutée. Chaque type motivationnel regroupe des items ou valeurs simples qui les représentent (soit 45 items au total), et qui ont une signification cohérente avec les différences culturelles intra-pays. Enfin, le modèle de Schwartz a fait l'objet d'évolutions : cf. Figure 20 page suivante.

Tableau 22 : 10 types motivationnels de Schwartz et les valeurs simples correspondants (Schwartz, 2006)

10 types motivationnels	Définition	Valeurs simples qui les représentent (Schwartz, 2006, p.964)
Pouvoir	Statut social et prestige, contrôle et domination des personnes et des ressources	Pouvoir social, Richesse, Autorité Préservant mon image publique Reconnaissance sociale
Accomplissement, Réussite	Réussite personnelle, liée à une compétence reconnue par les normes sociales	Ambitieux, Influent Compétent, Orienté vers le succès Intelligent
Hédonisme	Plaisir et gratification sensuelle envers soi-même	Plaisir Aimant profiter de la vie Se faire plaisir
Stimulation	Excitation, nouveauté et défi dans la vie	Vie passionnante, Vie variée Audacieux
Autonomie	Indépendance de pensée et d'action : choisir, créer, explorer	Liberté, Créativité Indépendant Choisissant ses propres buts Curieux, Vie privée Amour propre
Universalisme	Compréhension, appréciation, tolérance et protection de tous les hommes et de la nature	Égalité, Paix dans le monde Unité avec la nature Sagesse, Monde de beauté Justice sociale Harmonie intérieure Large d'esprit Protégeant l'environnement
Bienveillance	Préservation et amélioration du bien-être des personnes avec lesquelles on se trouve fréquemment en contact	Loyal, Honnête Responsable, Sens de la vie Pardonnant, Serviable Amitié vraie Amour adulte Vie spirituelle
Tradition	Respect, engagement et acceptation des coutumes et des idées préconisées par la culture traditionnelle et la religion	Respect pour la tradition Modéré Humble Détachement Pieux
Conformité	Modèle les actions, les possibilités de blesser/contrarier les autres, et de transgresser les attentes ou les normes sociales	Politesse Autodiscipline Honorant ses anciens Obéissant
Sécurité	Sécurité, harmonie et stabilité de la société, des relations et de soi	Ordre social, Sécurité nationale Réciprocité des services rendus, faveurs Sécurité familiale, Propre Sentiment d'appartenance Bonne santé

Figure 20 : Nouveau système des 19 valeurs de Schwartz (Schwartz et al., 2012)⁷⁹



Cette nouvelle version du modèle de Schwartz autour de 19 valeurs (Schwartz et al., 2012) ajoute deux axes : orientation vers le monde (focus social) vs vers soi (focus personnel) et motivation pour l'autoprotection vs pour recherche de la croissance. Les valeurs sont précisées et détaillées afin de gagner en fiabilité dans leur caractère prédictif d'attitudes et de comportements.

Ce modèle a servi de base à l'élaboration du Portrait Value Questionnaire dont l'objectif est de permettre l'identification des valeurs principales d'une personne. Nous en reparlons dans le paragraphe suivant.

⁷⁹Graphe disponible à : <http://www.psychomedia.qc.ca/psychologie/2016-02-04/19-valeurs-fondamentales-de-schwartz>

Enfin, les valeurs de Schwartz (1999, 2006) sont étudiées à un niveau individuel, et propose un modèle de dimensions culturelles plus individuel et plus dynamique que celui le modèle des dimensions nationales d'Hofstede que nous allons voir par la suite. Ainsi la théorie de Schwartz permettrait de mieux expliquer le comportement du consommateur (Steenkamp, 2001). Par ailleurs, Schwartz différencie des valeurs orientées vers des buts individuels (e.g., autonomie, hédonisme) et des valeurs orientées vers des buts collectifs (e.g., bienveillance, bénévolat), certaines étant entre les deux : ce que nous avons distingué entre objectifs individuels, collectifs ou mixtes dans la Figure 19.

Enfin, partant de la théorie des besoins de Maslow (1954, 1943), Bilsky & Schwartz (1994) distinguent les valeurs entre besoins de carence (e.g., Pouvoir, Sécurité) et besoins de croissance (e.g., Autonomie). Cette distinction est également faite sur la Figure 19. Les valeurs des besoins de croissance (e.g. vie privée) ne peuvent pas être activées si les valeurs des besoins de carence ne sont pas satisfaites. Ceci nous semble très important dans le cas de notre recherche où la protection des données personnelles est souvent associée à « un problème de riches »⁸⁰ et reliée à des dimensions d'individualisme, liée au développement économique et confort matériel.

⁸⁰ <https://linc.cnil.fr/fr/la-protection-des-donnees-est-elle-un-sport-de-riches>

3.4.3. Valeurs culturelles de Schwartz et comparaison avec les dimensions d'Hofstede

Schwartz a étudié la relation entre valeurs individuelles et cultures nationales. Ces valeurs servent ainsi à la grande étude *European Social Survey*⁸¹, questionnaire qui inclue 21 mesures d'items des valeurs humaines définies par Schwartz. Les 7 valeurs « culturelles » telles qu'identifiées par Schwartz sont (Schwartz, 1994b): (i) Autonomie intellectuelle et/ou affective vs. Conservatisme, (ii) Égalitarisme vs. Hiérarchie et (iii) Harmonie vs Maîtrise. Ces différenciations sont proches de celles d'Hofstede. De Mooij (2017) compare les dimensions culturelles d'Hofstede et de Schwartz, comme indiqué dans le Tableau 23.

Tableau 23 : Comparaison des dimensions culturelles d'Hofstede et de Schwartz (De Mooij, 2017)

Hofstede	Schwartz
Individualisme	Autonomie intellectuelle (liberté, curiosité, créativité, ouverture d'esprit) et autonomie affective (plaisir, jouissance de la vie, vie passionnante)
Collectivisme	Appartenance au groupe (« embeddness ») et conservatisme (tradition, ordre social, sécurité familiale, obéissance, réciprocité des faveurs),
Power distance	Hiérarchie (Humble, pouvoir social), Égalitarisme étant à l'opposé (égalité, honnêteté, loyal, responsable, serviable)
Masculinité	Maîtrise (Capable, audacieux, réussi, ambitieux, influent, reconnaissance sociale) étant à l'opposé d'Harmonie (protéger l'environnement, unité avec la nature, monde en paix, monde de beauté).

Cependant, comme nous l'avons précédemment évoqué, nous ne considérons pas que certaines valeurs sont plus culturelles que d'autres, et le terme « culturel » dans le cas ci-dessus nous semble utilisé pour faire des comparaisons entre pays.

⁸¹ <https://www.europeansocialsurvey.org/>

3.5. Diversité et pertinence de nouvelles approches de valeurs

D'autres modèles ont été proposés dans la continuité de celui de Schwartz, permettant de : (i) dresser le portrait d'une personne, (ii) prédire des attitudes ou comportements, (iii) comparer des cultures et mesurer des distances culturelles (i.e., degrés de similitude ou différence entre des cultures nationales ; Kogut and Singh's, 1988). Nous n'avons pas pour objectif de les détailler mais nous citons pour exemples le Basic Value Survey (Gouveia et al., 2008) ou le Social Value Orientation scale (Van Lange et al., 1997).

Ces modèles diffèrent sous certains aspects, notamment le nombre de valeurs mobilisées (e.g., deux valeurs pour Inglehart (1977) vs. 19 types de valeurs pour Schwartz et al. (2012) (Hanel et al. ; 2018), et les recherches se sont surtout intéressées aux différences entre les modèles. Cependant, ces valeurs, bien que nommées différemment, peuvent se rapprocher : e.g., « autonomie vs. sécurité/tradition » de Schwartz est proche de « individualisme-collectivisme » d'Hofstede et « laïque-rationnel » d'Inglehart (de Mooij, 2017; Kaasa, 2021). Ainsi Kaasa (2021) propose un modèle regroupant les ensembles de dimensions de Schwartz, d'Hofstede et d'Inglehart, à travers cela, montre qu'ils couvrent des gammes similaires de concepts.

De cette diversité de modèles émerge deux questions majeures :

- Quel modèle est le meilleur prédictif ? plusieurs études confirment la fiabilité du système de Schwartz et al. (2012), permettant soit d'anticiper des comportements prosociaux et pro-environnementaux (Hanel et al., 2018), soit de mesurer des distances culturelles (Imm Ng et al., 2007) ;
- Ces modèles sont-ils encore valables dans un contexte changeant, marqué par exemple par une baisse de la confiance dans les marques (Rajavi et al., 2019) ou encore un fort regain d'intérêt pour la consommation locale ? Les recherches montrent alors que ces modèles restent pertinents pour identifier dans quelle mesure les traits de personnalité ou les préférences culturelles peuvent influencer les effets d'actions marketing (Rajavi et al., 2019). Mais ce contexte invite à élargir les cadres conceptuels de compréhension des phénomènes (e.g., *consumer culture theory*, *acculturation theory*) afin de mieux identifier les corrélations entre les niveaux national, local/régional et individuel (Steenkamp, 2019). Ceci s'inscrit dans la démarche multi-niveaux de notre recherche que nous précisons par la suite.

3.6. Retours critiques sur les différents modèles de valeurs culturelles

3.6.1. Critiques possibles du modèle d'Hofstede

Le modèle d'Hofstede est le modèle référent pour la mesure de la culture nationale (Girerd-Potin et al., 2017), le plus utilisé par la recherche en marketing (De Mooij, 2017), et est massivement mobilisé dans les recherches sur l'influence de la culture sur la préoccupation pour la protection des données personnelles (e.g., Miltgen & Peyrat-Guillard, 2014). Nous insistons sur le fait que ces recherches apportent un éclairage précieux sur la compréhension de notre sujet. Nous ajoutons également que l'approche d'Hofstede est intéressante dans une perspective globale, nationale et institutionnelle. Dans ce contexte, nous décidons de la réutiliser dans notre premier essai.

Cependant, le modèle d'Hofstede est également le plus critiqué (e.g., Jones, 2007 ; Ailon, 2008). Il nous est nécessaire d'en maîtriser les raisons. En effet, le modèle d'Hofstede est considéré comme un « concept de culture fragile et surutilisée, opérationnalisation discutable, ethnocentrisme sous-jacent, lié à une recherche principalement occidentale en langue anglaise » (Livian, 2011, p.1) ainsi que ses limites méthodologiques (Mc Sweeney, 2002). Il lui est reproché :

- De limiter la culture avec des frontières restreintes et d'utiliser des moyennes nationales pour représenter des scores individuels, en ignorant l'existence de sous-cultures sous-jacentes ;
- De surestimer la stabilité des cultures et des identités, basée sur un déterminisme culturel sans aucune place pour les cultures mixtes ou coconstruites ;
- De considérer la culture avec un ethnocentrisme sous-jacent (i.e., l'utilisation de sa propre culture comme norme pour juger les autres cultures), avec une recherche occidentale essentiellement en anglais, et un référentiel culturel fixe, donc potentiellement déguisant une idéologie puissante. Par exemple le modèle est basé sur des représentations occidentales du pouvoir ou de la distance hiérarchique, donnant pour des pays comme le Japon des résultats surprenants ;
- De mesurer la culture en intégrant des limites : précisions des données mesurées par questionnaires, correspondances interculturelles, biais liés à de variations de degrés de conformité au groupe. Pour cela, des approches qualitatives doivent être développées.

Nous retenons de ces critiques que le modèle d'Hofstede est approprié pour étudier les différences de cultures nationales, mobilisant des scores à un niveau national, et en l'appliquant à des pays européens et occidentaux. En revanche, les dimensions de la culture nationale peuvent plus difficilement être utilisées au niveau individuel (Oyserman et al., 2002) et l'application des échelles nationales au niveau individuel pose problème (Brewer & Venaik, 2012). Nous prenons en considération les différentes critiques pour proposer une approche dans notre thèse qui y réponde.

3.6.2. *Réflexions sur l'ensemble des modèles existants*

De façon générale, tout modèle présente des avantages mais également des inconvénients. Par exemple, le modèle de Schwartz fait à nouveau appel à un prisme très occidental. Il nous paraît assez complexe à opérationnaliser : le nombre de valeurs à tester implique un questionnaire assez long. Le modèle de Triandis est intéressant mais trop réducteur pour prendre en compte toutes les valeurs possibles. Tous les systèmes de valeurs doivent être utilisés avec prudence, afin d'éviter la tentation d'une utilisation facile des statistiques pour expliquer un phénomène profond.

En revanche, la triangulation de différentes approches est fructueuse :

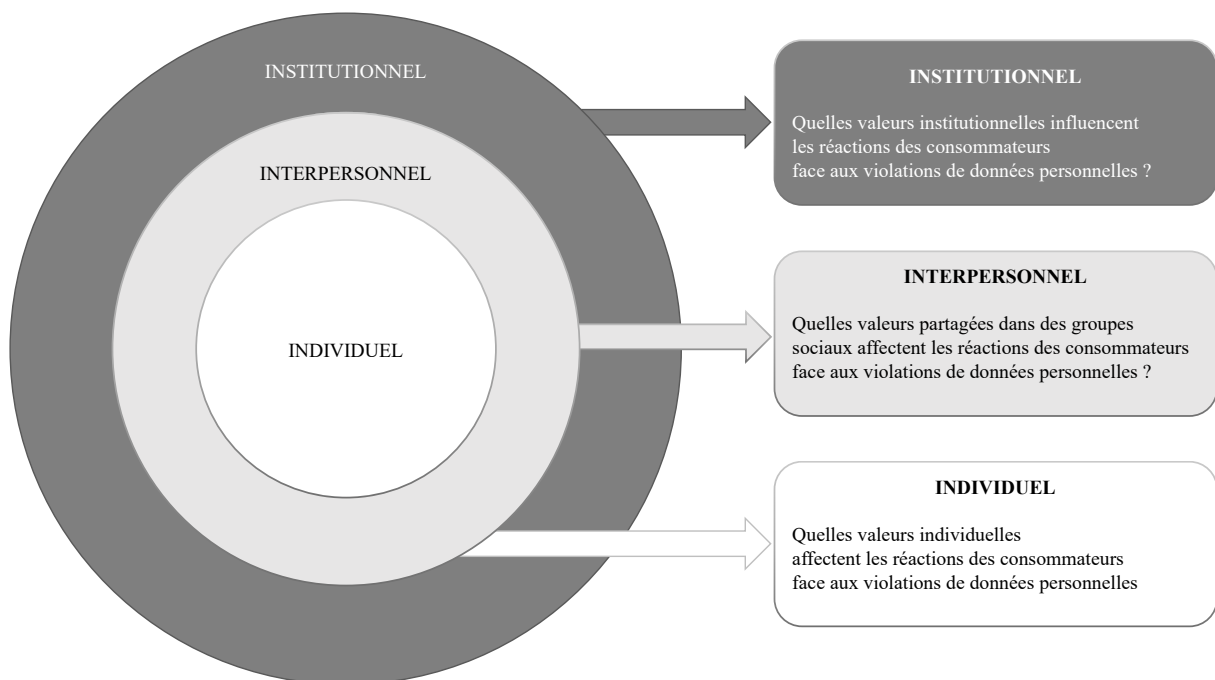
- Pour cela, notre thèse propose d'articuler les niveaux d'analyse macro (global et national), méso (organisation, groupe, secteur) et micro (individuel) ;
- Elle adopte des approches déductives (essai 1 et 3) et inductive (essai 2) ;
- Dans notre essai 2, nous nous autorisons de ne faire appel à aucun modèle précis.

3.6.3. *Nécessité d'une approche macro, méso et micro*

Comme nous venons de le voir, les chercheurs en management interculturel (e.g., Livian, 2011) conseillent une approche multi-niveaux pour mieux rendre compte de la compréhension des effets culturels. Les chercheurs en marketing international (Akaka et al., 2013) ainsi que les chercheurs en protection de la vie privée conseillent également cette approche. Les recherches portent généralement sur 2 niveaux : macro et micro (que nous présenterons ci-dessous alors en premier), et soulignent ensuite la nécessité de prendre en compte un troisième niveau intermédiaire (le niveau méso). Nous adoptons une approche à trois niveaux : macro, méso et micro, que nous précisons dans le chapitre 3 suivant.

Appliqué à notre sujet, la protection des données personnelles est intégrée au sein de nos institutions par le RGPD, et est ensuite véhiculée par exemple au sein des entreprises : les individus acquièrent les bonnes pratiques et développent une sensibilisation à ce sujet dans leur sphère professionnelle. Notre question est de savoir quelles sont les valeurs qui agissent aux niveaux institutionnel (macro), interpersonnel (méso) ou individuel (micro). Nous précisons ces questions dans la Figure 21 ci-dessous.

Figure 21 : Niveaux institutionnel, interpersonnel et individuel



Synthèse de la section culture et valeurs culturelles

Trois points sont à retenir de cette revue de littérature sur la culture, pour la suite de notre recherche.

Premièrement, la culture est une conscience collective constituée de valeurs, propres à un pays, à un groupe social (e.g., une génération), et spécifique à chaque individu. Les valeurs portent la culture et sont des symboles qui donnent du sens à la décision et à l'action. C'est pourquoi tout phénomène social est culturel car il est l'expression de valeurs partagées. Enfin, la culture est fixe dans le temps, change peu, alors que le contexte est variable : la culture agit comme un kit d'interprétation d'éléments contextuels.

Deuxièmement, les valeurs sont des idéaux qui guident la décision et l'action : e.g., un idéal de sécurité, ou un idéal de fraternité. Ces valeurs sont à la fois universelles et implicites. Elles sont acquises par des processus de socialisation, par l'intégration d'habitus. Enfin, elles interviennent à un niveau macro (elles sous-tendent nos lois), méso (elles cimentent les relations sociales et les organisations) et micro (psychologiquement).

Troisièmement, aucun modèle de valeurs culturelles n'est parfaitement correct et juste. Une bonne compréhension des effets culturels nécessite une approche multi-niveaux (macro, méso et micro) et la triangulation de méthodologies (déductive et inductive) et de données.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

Protection
des données
personnelles

Réponses des
consommateurs
insatisfaits

Culture
et valeurs



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :
Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :
Influence des
normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :
Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 3. Cadre général de la thèse



Nous retenons des deux précédents chapitres trois idées centrales : (i) le souci de protection de ses informations personnelles est un concept abstrait ; (ii) les réponses face à une violation de données personnelles peuvent faire appel à d'autres antécédents tels que le sentiment de capacité individuelle ou la pression sociale à agir ; (iii) la culture est une conscience collective composée de valeurs, socle de nos décisions, actions et institutions, au-delà de toutes frontières nationales.

Ce troisième chapitre a pour vocation d'exposer comment nous allons utiliser ces trois idées pour répondre à notre question de recherche, c'est-à-dire : quelle est l'influence de la culture sur les réponses face à une violation de ses données personnelles ?

La première section synthétisera les idées extraites de notre revue de littérature sur lesquelles se fonde notre thèse. Nous exposerons notre modèle conceptuel selon trois niveaux d'observation (macro, méso et micro). La deuxième section expliquera notre posture épistémologique, post-positiviste, socle de notre approche méthodologique. La troisième section, exposera la structure générale de la thèse ainsi que l'apport de chacun de nos 3 essais.

Section 1. Questions de recherche et cadre théorique général

1. Synthèse du contexte et des fondements théoriques

En 2021, seuls 20% des entreprises ont déclaré ne pas avoir été attaquées informatiquement⁸² et 952,8 millions de personnes ont été victimes d'une violation de données personnelles dans le monde⁸³. En parallèle, des réglementations pour la protection des données personnelles se mettent en place dans différents pays (e.g., RGPD, CPRA, PIPL, PDPB) mais sont adoptées différemment par les individus, en témoignant la forte variabilité du nombre de plaintes déposées aux autorités de protection des données personnelles en Europe⁸⁴. Malgré ces tendances, les recherches examinant les réactions des consommateurs à l'égard des violations de données personnelles et leurs attentes sont peu explorées (Labrecque et al., 2021). En outre, les résultats contradictoires obtenus par les recherches portant sur l'influence de la culture sur la préoccupation pour la protection de la vie privée appellent de nouvelles explorations (e.g., Martin et al., 2020).

Nous retenons trois idées phare de notre revue de la littérature : (i) importance du souci de contrôle de ses informations personnelles comme antécédent aux réponses face à une violation de ses données personnelles mais concept abstrait ; (ii) importance d'autres antécédents dans le comportement de réponse face à une violation de données tels que l'auto-efficacité et la pression sociale ; (iii) considération de valeurs culturelles, socle des actions et des institutions.

Les points clés de notre revue de littérature figurent dans le Tableau 24.

⁸² Acronis Cyberthreats Report 2022. *op. cit.*

⁸³ <https://www.lebigdata.fr/violation-de-donnees-2021PBPA>

⁸⁴ DLA Piper GDPR fines and data breach survey. *op. cit.*

Tableau 24 : Synthèse des fondements théoriques de la thèse

Souci de contrôle de ses données personnelles (SCDP)	1. Le SCDP repose sur le droit des individus de contrôler l'accès et l'usage de leurs données personnelles, et sur un principe de contrat social entre un individu et une entreprise qui collecte les données. Ainsi les proxys utilisés pour évaluer la SCDP sont définis autour de dimensions de contrôle et de transparence. 2. Le SCDP intervient dans les arbitrages institutionnels et réglementaires (macro), économiques et organisationnels (méso), psychologiques (micro). 3. Dans un contexte d'usage et de collecte explosive de données personnelles, la SCDP fait l'objet de débats car est une notion abstraite donc prise artificiellement en considération dans les arbitrages des individus, générant des situations paradoxales entre un souci de protection déclaré et un comportement réel, avec un impact sur la vulnérabilité du consommateur (d'autant plus importante dans le cas de violations de données personnelles). De ce fait, la SCDP fait l'objet de nouvelles conceptualisations et des recherches explorent le rôle de la distance psychologique avec les risques liés à la vie privée. 4. Une meilleure compréhension des intentions comportementales face à une violation de données personnelles et des mécanismes reliant valeurs et réponses implique de mieux comprendre le rôle la SCDP, qui peut être un antécédent mineur face à d'autres facteurs sociétaux (e.g., pression sociale) dans les réponses apportées.
Réponses des consommateurs insatisfaits (RCI)	1.1.1 Les RCI sont des tentatives de clients de modifier une situation insatisfaisante, qui passent par des phases d'évaluation psychologique, de capacité sociétale, d'évaluation du cadre juridique et de stratégies de réponse : une compréhension des RCI doit passer par une analyse à des échelles macro, micro, méso. 2.1.1 Les RCI peuvent être absentes, privées ou publiques. Dans le cas d'une violation de leurs données personnelles, elles peuvent être techniques, sociales, institutionnelles. 3.1.1 Les RCI ont des antécédents tant psychologiques que sociétaux (e.g., self-efficacy et rôles sociaux).
Culture	1. La culture est un ensemble de valeurs universelles et implicites, acquises par des processus de socialisation, propres à un pays, à un groupe social et spécifique à chaque individu. Les valeurs portent la culture, i.e., les symboles qui donnent du sens, et ce en dehors de toute frontière nationale. 2. Les valeurs voyagent entre un cadre institutionnel (macro) et un psychisme individuel (micro) par des processus de socialisation, de mimétisme et de <i>practice</i> (méso). Ces valeurs sont le socle des réglementations, des choix organisationnels, des actions marketing et de communication. Elles impulsent les choix et les actions de chaque individu. 3. Parmi ces valeurs, l'individualisme est une vision du monde à portée politique forte, une norme macro, fondatrice de la théorie du contrat social. 4. Aucun modèle de valeurs culturelles n'est parfaitement correct et juste. Une bonne compréhension des effets culturels nécessite une approche multi-niveaux et la triangulation de méthodologies et de données.

2. Trois niveaux d'observation : macro, méso et micro

2.1. Théorie des échelles d'observation (Desjeux, 2006)

Nous avons montré l'importance d'adopter une approche des effets culturels multi-niveaux : macro, méso et micro. Ces trois niveaux d'observation peuvent aussi être nommés : institutionnel, interactionnel et individuel. En effet, la protection des données personnelles est un enjeu sociétal qui touche tant les institutions, les organisations et les individus. Les réactions des consommateurs insatisfaits suivent un processus diachronique mobilisant des évaluations conative, cognitive et affective à différents niveaux (institutionnel, organisationnel, personnel).

En sciences sociales, Desjeux (2006) conseille d'appliquer la théorie des échelles d'observation pour la compréhension des phénomènes sociaux et la rationalité des acteurs, notamment en démographie compréhensive. Il propose 4 niveaux d'analyse :

- le macro-social (défini par la classe sociale, la génération, le genre, la culture),
- le méso-social (défini selon les organisations, les relations de pouvoir ou d'intérêts),
- le micro-social (défini selon les sphères privées ou domestiques),
- le micro-individuel (défini par une échelle d'approches cognitives ou psychologiques).

Pour apprécier correctement un phénomène social (e.g., les réponses face à une violation de données personnelles), la diversité des niveaux d'observation est fondamentale car « *ce qui est visible à une échelle disparaît quand on change d'échelle d'observation, mais d'autres aspects ou d'autres phénomènes invisibles à l'échelle précédente apparaissent du fait de ce changement d'échelle* » (Desjeux, 2006, p.14).

Nous adoptons alors une approche à trois niveaux : macro, méso et micro, que nous précisons ci-dessous (en particulier le niveau méso qui est le moins souvent mobilisé). Les recherches portent généralement sur 2 niveaux : macro et micro (que nous présenterons ci-dessous alors en premier), et soulignent ensuite la nécessité de prendre en compte un troisième niveau intermédiaire (le niveau méso).

2.2. Niveau macro

Le niveau macro correspond en management des organisations aux effets externes à l'organisation : i.e., facteurs politiques et économiques, systèmes juridiques, société dans son ensemble.

Au niveau macro, les valeurs se déclinent au niveau des institutions. Rokeach (1979) parle de valeurs « supra-individuelles », i.e., valeurs institutionnelles, organisationnelles, idéologiques, évoluant sur le temps long et historique. Par exemple, les lois pour le droit à l'avortement ou le mariage pour tous résultent de changements de valeurs lents et profonds. Les institutions sont « des arrangements sociaux qui fournissent les cadres pour la spécialisation des valeurs, qui sont principalement les cadres pour la transmission et la mise en œuvre de ces séries de valeurs qui sont spécialement impliquées dans leurs propres sphères particulières d'activités » (Rokeach, 1979, p.51). Les institutions peuvent être l'école, institution forte de transmission de valeurs (avec des choix importants comme le port du voile), mais aussi les médias, qui sont des importants agents de socialisation, inculquant valeurs, idéologies et attitudes (Maio et al., 2006). Ces normes sont également considérées comme des hyper-normes (Donaldson & Dunfee, 1994), convergence de valeurs religieuses, philosophiques et culturelles à travers lesquelles une question éthique est évaluée, telles que la vie privée. L'évolution des valeurs entraîne l'évolution du cadre juridique (Bréchon, 2019).

2.3. Niveau micro

Le niveau micro correspond en management des organisations au niveau individuel.

Au niveau micro, les valeurs agissent au niveau des processus psychologiques pour distinguer le vrai du faux, le bon du mauvais. Ce sont des idées et croyances partagées d'une culture. Cependant les valeurs sont des concepts plus sociologiques que psychologiques (Rokeach, 1979). Les valeurs s'expriment à un niveau individuel comme des représentations cognitives des besoins personnels et les moyens de les satisfaire, mais résultent avant tout de constructions sociales et institutionnelles.

2.4. Niveau méso

Le niveau méso correspond en management à des organisations aux effets internes à l'organisation (notamment à des niveaux intermédiaires de management). Le niveau méso est le lieu des interactions interpersonnelles (Matsumoto, 2007), incluant les familles, les gouvernements, les systèmes éducatifs, les organisations sportives, les groupes religieux, et tout autre groupe. Au niveau méso, les valeurs véhiculées par les institutions sont transmises au sein des groupes sociaux par des phénomènes de mimétisme et de transmission d'*habitus* (i.e., l'internalisation permanente de l'ordre social dans le corps humain). En effet, pour déterminer un ordre social, les règles institutionnelles (i.e., « venues d'en haut ») ne suffisent pas. Elles doivent être adoptées par la société, grâce à un ensemble d'apprentissages peu à peu intégrés par les individus eux-mêmes, permettant une adhésion collective aux principes édictés (Maisonneuve, 2017).

Il apparaît d'autant plus essentiel de s'interroger sur les réponses de protection de la vie privée à un niveau méso, que la décision d'agir pour la protection de la vie privée résulte souvent d'un compromis entre une action civique (*civic agency*), en tant que citoyens, et une action quotidienne (*market agency*) en tant qu'acteurs ou consommateurs (Chaudhury & Albinsson, 2015). Cette tension citoyen-consommateur se situe entre les macro-pouvoirs des institutions (contrôle de la réglementation de la protection des données personnelles et de l'économie numérique), et le micro-pouvoir individuel (gestion des données personnelles).

Elle se traduit par un écart entre les besoins de la société au niveau macro et ceux des consommateurs au niveau micro (Valor et al., 2017). Ne pouvant avoir une influence immédiate et réelle au niveau macro (réglementation et économie numérique), les individus cherchent à avoir un rôle au niveau méso (e.g., groupes sur les réseaux sociaux pour échanger des trucs et astuces pour se protéger en ligne, ou les associations militantes). En particulier, les changements sociétaux résident essentiellement dans les liens de causalité à un niveau méso (Johnson & Schaltegger, 2020) et les associations et les groupes sociaux contribuent aux orientations de la société, par le développement d'idées et de référentiels, et où des dynamiques collectives se développent (Chognot, 2020).

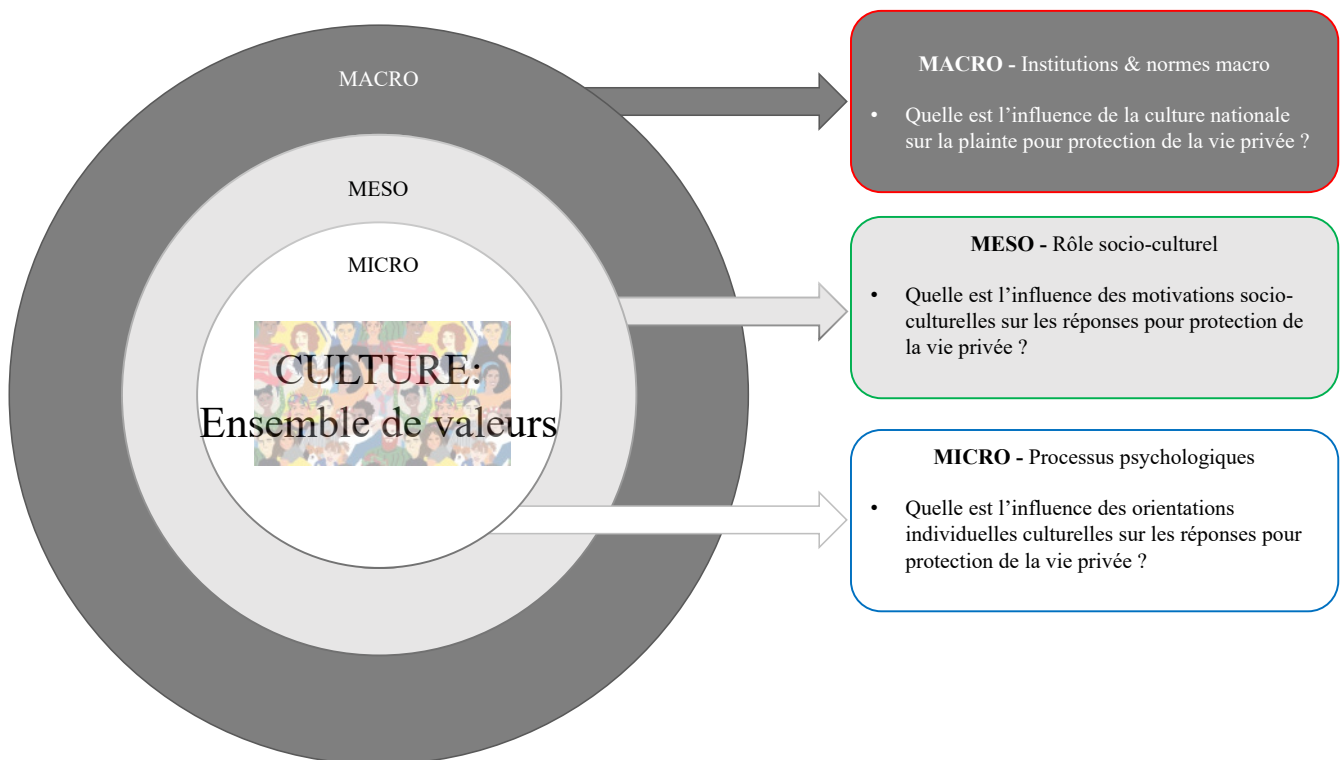
Plusieurs actions menées par les régulateurs nationaux en matière de protection de la vie privée sont initiées par des collectifs comme la Quadrature du Net en France ou NOYB (« *None Of Your Business* ») pilotée par l'autrichien Marx Schrems, qui a permis d'invalider en juillet 2020

le Privacy Shields (i.e., l'accord de compatibilité des réglementations de protection permettant le transfert de données personnelles de citoyens européens vers les États-Unis) ou de rendre illégale début 2022 en Europe l'utilisation de Google Analytics (pour des raisons de non-conformité au RGPD).

2.5. Trois niveaux au regard de notre question de recherche

Notre question de recherche principale « Quelle est l'influence de la culture sur les comportements de réponses face à une violation de données personnelles ? », est considérée en trois étapes (cf. Figure 22) : influence des dimensions de la culture nationale, influence des motivations socio-culturelles, influence des orientations culturelles individuelles. Nous obtenons trois questions de recherche :

Figure 22 : Trois niveaux d'observation de l'influence de la culture



La première question « **Quelle est l'influence de la culture nationale sur la plainte du consommateur pour protection de sa vie privée ?** » vise à identifier les dimensions de la culture nationale qui impactent le comportement de plainte, et à comprendre conceptuellement le lien entre ces dimensions et les normes institutionnelles sur lesquelles repose le contrat social autour de la collecte et de l'usage des données personnelles, influençant la compréhension des menaces possibles apportées à la vie privée.

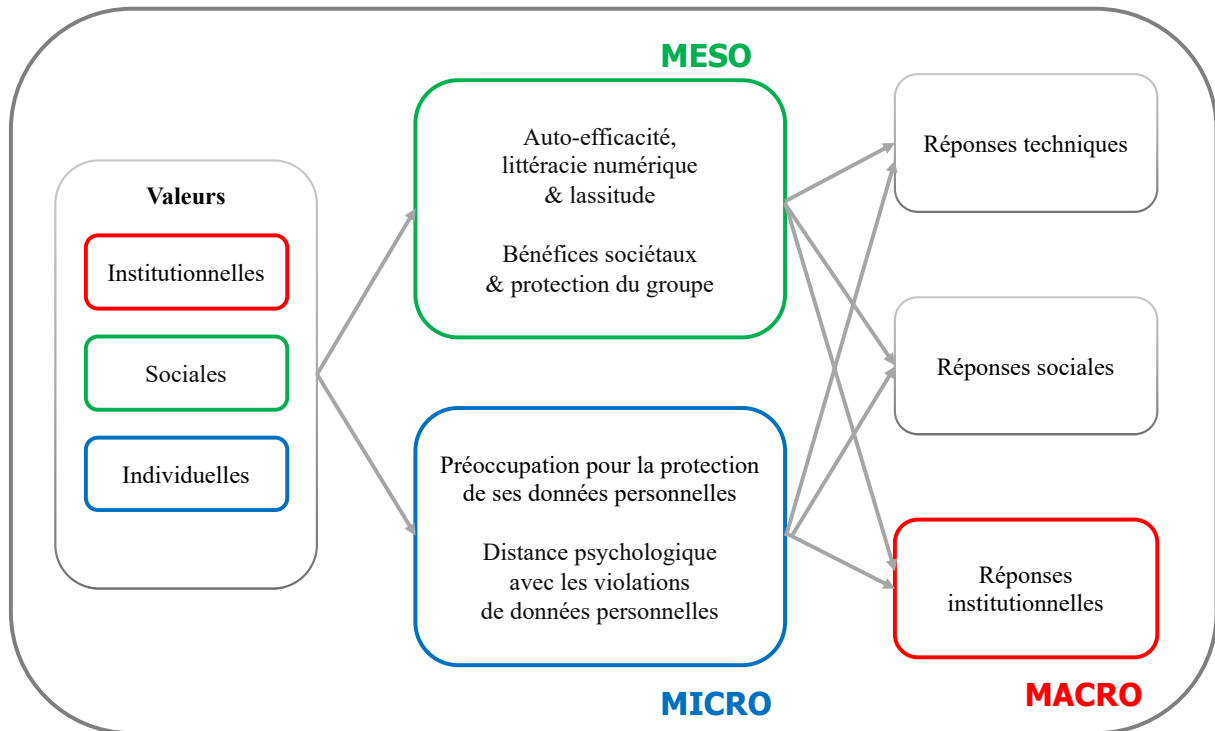
La deuxième question « **Quelle est l'influence des motivations socio-culturelles sur les réponses du consommateur face à une violation de ses données personnelles ?** » vise à identifier les normes socio-culturelles partagées au sein d'un groupe et transmises entre pairs, ainsi qu'à éclairer les mécanismes sociétaux et les modèles de motivation à répondre à une violation de ses données personnelles. Nous mobiliserons la *practice theory* (Bourdieu, 1972; Giddens, 1979) pour éclairer ces questions. D'autres antécédents pourront être identifiés (*self-efficacy*, bénéfices sociétaux, normes subjectives). Cette recherche nous permettra de préciser encore les types de réponses face à une violation de données personnelles.

La troisième question « **Quelle est l'influence des orientations culturelles individuelles sur les réponses du consommateur face à une violation de ses données personnelles ?** » vise à identifier les valeurs et orientations culturelles psychologiques et individuelles en jeu, ainsi qu'à éclairer les mécanismes psychologiques reliant les valeurs culturelles et les réponses du consommateur face à une violation de ses données personnelles. Nous mobiliserons alors la théorie de la distance psychologique (Trope & Liberman, 2010) ainsi que le souci pour la protection de ses données personnelles pour éclairer la représentation psychologique de ce qui peut être violé et de comment cela peut être violé. Cette recherche nous permettra également de préciser les types de réponses face à une violation de données personnelles.

3. Modèle conceptuel

Nous obtenons alors le modèle conceptuel présenté dans la Figure 23.

Figure 23 : Modèle conceptuel de la thèse



Chaque niveau d'analyse mobilise un cadre théorique que nous reprenons dans le Tableau 25.

Tableau 25 : Cadres théoriques utilisés dans la thèse

Culture : Réponses :	MACRO (Institutionnel)	MÉSO (Rôle socio-culturel)	MICRO (Processus psychologiques)
Compréhension de la menace	Social contract theory		
Évaluation sociétale		Social practice theory	
Évaluation psychologique	-		Construal level theory

Section 2. Positionnement épistémologique et méthodologies de recherche

« Tout travail de recherche repose sur une certaine vision du monde, utilise une méthodologie, propose des résultats visant à comprendre, expliquer, prédire ou transformer. Une explicitation de ces présupposés épistémologiques permet de contrôler la démarche de recherche, d'accroître la valeur de la connaissance qui en est issue, mais également de mieux saisir nombre de débats entre courants théoriques en management » (Allard-Poesi & Perret, 2014, p.14).

Notre recherche repose sur un **positionnement épistémologique post-positiviste**. Le positionnement post-positiviste est un juste équilibre entre approches positiviste et interprétativiste (Cooper, 1997). Nous allons tout d'abord expliquer ce qui différencie positivisme et interprétativisme (1), pour ensuite préciser les fondements du post-positivisme (2). Nous expliquerons pourquoi nous adoptons cette approche et détaillerons comment cela se traduit méthodologiquement dans notre thèse (3).

1. Différence entre positivisme et interprétativisme

Le positivisme considère que la théorie précède l'expérience (Popper, 1959) : l'objet de recherche doit donc être défini théoriquement, puis les hypothèses de recherche doivent être validées empiriquement, en utilisant des approches hypothético-déductives et généralement des méthodes quantitatives. À l'opposé, pour la recherche exploratoire et interprétativiste, la réalité ne peut être appréhendée qu'à travers une implication du chercheur permettant de donner sens aux expériences dans un contexte donné (Denzin & Lincoln, 2008), s'appuyant principalement sur des approches qualitatives. Weber (2004) détaille ces principes sur plusieurs niveaux (ontologie, épistémologie, définition des objets de recherche, méthodes, théorie de la vérité, validité et fiabilité) et montre comment positivisme et interprétativisme se différencient tant sur des hypothèses métathéoriques que des paradigmes de recherche : cf. Tableau 26.

Tableau 26 : Hypothèses métathéoriques et paradigmes de recherche (Weber, 2004)

	Positivisme	Interprétativisme
Ontologie	La personne (le chercheur) et la réalité sont séparées.	La personne (le chercheur) et la réalité sont inséparables (<i>life-word</i>)
Épistémologie	La réalité objective existe au-delà de l'esprit humain.	La connaissance du monde est intentionnellement constituée par l'expérience vécue d'une personne.
Objet de recherche	L'objet de la recherche possède des qualités inhérentes qui existent indépendamment du chercheur.	L'objet de la recherche est interprété à la lumière de la structure de signification de l'expérience vécue par la personne (le chercheur).
Méthode	Statistiques, analyse du contenu.	Herméneutique, phénoménologie, etc.
Théorie de la vérité	Théorie de la correspondance de la vérité : mise en correspondance un à un entre les énoncés de recherche et la réalité.	La vérité en tant que réalisation intentionnelle : les interprétations de l'objet de la recherche correspondent à l'expérience vécue de l'objet.
Validité	Certitude : les données mesurent réellement la réalité.	Des revendications de connaissances défendables.
Fiabilité	Reproductibilité : les résultats de la recherche peuvent être reproduits.	Conscience interprétative : les chercheurs reconnaissent et abordent les implications de leur subjectivité.

2. Approche post-positiviste

2.1. Définition du post-positivisme

Le post-positivisme repose sur l'idée principale qu'« il faut reconnaître qu'il n'existe pas de connaissance neutre : la connaissance ne peut pas être séparée de l'ontologie (*être*) et de l'expérience personnelle » (Ryan, 2006, p.16). L'approche post-positiviste soutient l'idée que le chercheur est influencé par son propre système de valeurs et un cadre général de pensée (i.e., une certaine vision du monde). Le post-positivisme remet en question l'objectivité du chercheur inhérente au positivisme : alors que le positivisme repose sur l'idée que le chercheur pose des hypothèses en se basant sur la théorie en toute indépendance, le post-positivisme soutient que cette indépendance n'existe pas et que le chercheur est influencé par ses valeurs, ses connaissances et son vécu (Robson, 2002). Le chercheur doit donc prendre conscience de ces biais axiologiques et chercher à les interroger, pour rechercher l'objectivité (Butori & Parguel, 2010).

Le post-positivisme n'est pas un rejet d'une méthode scientifique mais plutôt une reformulation du positivisme pour répondre à certaines critiques. Ainsi, le post-positivisme mobilise les fondements de base du positivisme, i.e., la possibilité d'une vérité objective, et l'utilisation de méthodologies quantitatives et expérimentales. En d'autres termes, une réalité objective existe, mais toute connaissance humaine est basée sur des conjectures, qu'il convient de justifier par un ensemble de garanties.

L'approche post-positiviste est née d'une approche critique de la recherche positiviste, en provenance des mouvements féministes, ethnographiques ou post-coloniaux, et conduit d'une certaine manière à une recherche critique (Ryan, 2006). Les paradigmes post-positivistes et critiques partagent certains fondements épistémologiques et ontologiques (Cooper, 1997). Notamment, selon Ryan (2006, p.12), « *les principes de la recherche post-positiviste mettent l'accent sur le sens et la création de nouvelles connaissances, et sont capables de soutenir des mouvements sociaux engagés, i.e., des mouvements qui aspirent à changer le monde et à contribuer à la justice sociale.* » Cependant l'approche post-positiviste est moins catégorique et plus ouverte à l'usage de différentes méthodes, l'approche critique indiquant que seules des méthodes objectives sont valables (Cooper, 1997).

2.2. Post-positivisme et cohérence avec mon approche personnelle

L'approche post-positiviste correspond à la manière avec laquelle j'ai toujours appréhendé le monde, tant dans ma vie professionnelle que dans ma vie personnelle.

De formation plutôt scientifique, j'ai une appétence particulière pour l'approche quantitative de mon environnement. J'ai été responsable d'études de marché en panels distributeurs, consommateurs et de mesure d'audience de médias pendant quinze ans. De plus, je considère que la découverte d'un nouvel environnement (nouveau secteur d'activités, nouveau pays, nouvelle culture) doit s'accompagner d'une lecture attentive des statistiques (e.g., évolution du niveau de vie ou des indicateurs de développement humain).

Cependant les études de marché les plus riches que j'ai conduites ont toujours été accompagnées d'un volet qualitatif (e.g., marché des lentilles de contact en France en 2006 ; nouvelles émissions TV marocaines en 2010) : le « pourquoi » venant enrichir le « combien ». Enfin et surtout, la connaissance et la compréhension d'un nouvel environnement culturel doivent selon

moi obligatoirement s'accompagner d'une immersion forte dans cet environnement. J'ai toujours cherché à pousser les limites de cette découverte, ce qui n'a pas été sans difficulté et conséquence. Ceci m'a permis de percevoir la réalité différemment, comme l'indique Hall (1976, p.21) : « *Grâce à mon expérience d'autres systèmes culturels, j'ai découvert que de telles contraintes s'exerçaient dans d'autres domaines que celui du langage. Naturellement, pour s'en apercevoir, il faut avoir eu la chance d'étudier d'autres cultures suffisamment différentes de sa propre culture pour mettre ses structures cachées en évidence.* »

2.3. Pertinence du post-positivisme pour notre sujet

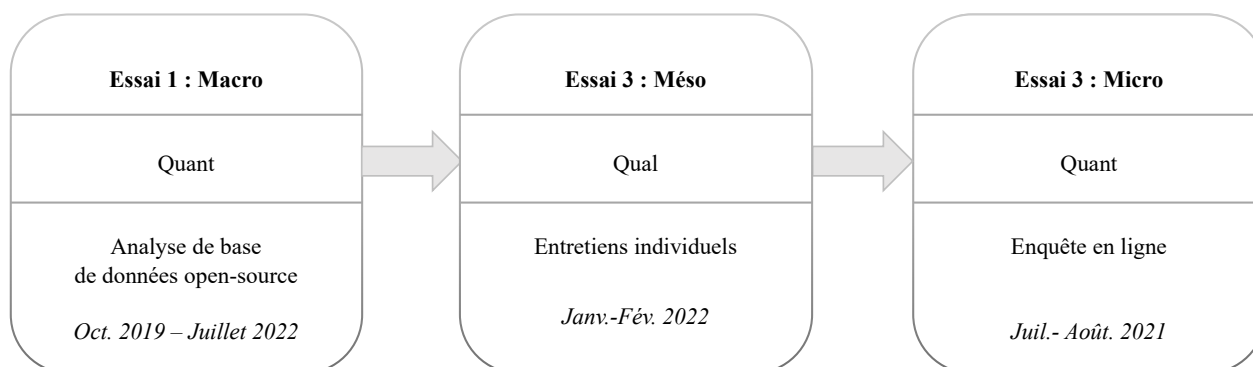
Alors que notre recherche s'inscrit dans un champ relativement nouveau (les comportements du consommateur face à une violation de ses données personnelles) qui appelle à sortir des schémas culturels existants, l'approche post-positiviste s'applique particulièrement bien à notre sujet.

3. Méthodologies de recherche

De ce positionnement post-positiviste découle une collecte de données tant quantitative que qualitative. Notre thèse de doctorat s'articule autour de trois approches empiriques (détaillées sur la Figure 24 et dans le Tableau 27) :

- Une première approche quantitative, basée sur l'analyse d'une base de données open-source (nous reconnaissons un certain opportunisme dans l'exploitation de ces données trouvées par hasard) ;
- Une deuxième approche qualitative, basée sur une série d'entretiens approfondis, nous permettant d'approfondir la compréhension de certains phénomènes de réponses pour la protection de données personnelles face à une violation de données ;
- Une troisième approche quantitative, hypothético-déductive, qui a confirmé nos premiers résultats.

Figure 24 : Processus de collecte de données



La compréhension des raisons de ces phases successives doit aussi être mise au regard du contexte de réalisation de notre recherche : d'une part, la nécessité d'une forte montée en maturité de chercheur, et d'autre part, les contraintes matérielles et psychologiques fortes liées à la crise sanitaire du Covid-19, vécue hors France. Ainsi les collectes de données ont aussi été réalisées au gré des opportunités que le contexte permettait.

Les collectes de données sont détaillées dans le Tableau 27 ci-après.

Tableau 27 : Détails des collectes de données réalisées dans chaque essai

	Essai 1 : Macro	Essai 2 : Méso	Essai 3 : Micro
	Influence de la culture nationale	Influence des normes socio-culturelles	Influence des orientations culturelles individuelles
Nature	Quantitative	Qualitative	Quantitative
Région, pays	Europe	France	France
Méthode de collecte de données	Base de données open-source	Entretiens individuels en profondeur	Questionnaire en ligne
Échantillon	25 pays	15 entretiens	452 participants
Mode de sélection	-	Essentiellement prise de contact direct sur Twitter, puis effets « boule de neige ». Quelques entretiens sollicités dans l'entourage direct de l'autrice	Aléatoire auprès d'un panel
Méthode d'analyse de données	Régression statistique	Analyse thématique et chaînage cognitif	Équations structurelles
Solutions software	IBM SPSS Statistics v21	NVivo v12 pour le codage cognitif	XL-STAT/PLSPM



Section 3. Structure de la thèse et apports de chaque essai

1. Description et objectifs de chaque essai

Notre thèse s’articule en trois essais, répondant à la question générale : « Quelle est l’influence de la culture sur le comportement de réponses face à une violation de données personnelles ». Ces essais correspondent respectivement aux niveaux macro, méso et micro, et à trois questions de recherche différentes : (i) quelle est l’influence de la culture nationale ? ; (ii) quelle est l’influence des normes socio-culturelles ? ; (iii) quelle est l’influence des orientations culturelles individuelles ?

Dans cette partie, nous présentons les résumés de chaque essai, un tableau (Tableau 28) comparant leurs apports respectifs, et incluant également les contributions de chacun des auteurs. Nous finissons par un résumé général de la thèse.

Notre thèse se conclut par un chapitre consacré à une discussion finale, permettant de détailler les contributions théoriques de notre recherche et d’identifier les mises en application possibles des résultats de notre recherche.

Résumé essai 1 (chapitre 4 – Macro) : L’Union européenne a adopté en mai 2018 le RGPD afin de renforcer la protection de la vie privée et des données personnelles des individus, d’harmoniser les différentes réglementations européennes et d’imposer des obligations aux organisations. Constatant une grande variance dans le nombre de plaintes déposées auprès des différentes autorités de protection des données personnelles en Europe depuis lors (e.g., CNIL en France), cette recherche examine l’influence de la culture nationale sur le comportement de plainte pour violation de la protection des données personnelles. S'appuyant sur le modèle de la culture nationale d’Hofstede (Hofstede, 1984, 2001; Hofstede et al., 2010), nous montrons que les individus issus de pays européens valorisant davantage la féminité (i.e., privilégiant l’égalité des genres et le soin apporté aux autres) portent davantage plainte pour la violation de données personnelles. Il en est de même mais dans une moindre mesure auprès des individus issus de pays européens valorisant davantage l’individualisme (i.e., une préférence pour une autonomie, indépendance et liberté individuelle, privilégiée à l’équilibre et la défense du groupe social – dimension opposée au collectivisme) ou la tradition.

Résumé essai 2 (chapitre 5 – Méso) : à partir d’entretiens approfondis (N=15), et à la lumière de la théorie de la pratique (Bourdieu, 1972; Giddens, 1984), nous montrons, d’une part, que la défense d’une équité sociale est une motivation essentielle à un engagement collectif pour le respect de la vie privée, et d’autre part, que la protection de la vie privée est une pratique sociale et collective. Cette pratique sociale se développe autour de structures mobilisant des valeurs (idéaux), des moyens (matériaux), et des compétences ou croyances (e.g., sentiment d’efficacité). Un développement équilibré entre idéaux, moyens et compétences permet l’adoption d’une réponse active face à une violation de données personnelles. Enfin, la défense soit de sa liberté, soit de son sécurité personnelle (à travers la protection de son autonomie et intimité) sont deux motivations supplémentaires à ces réponses. Cette recherche envisage la question de la protection de la vie privée comme une pratique sociale, et non comme une pratique individuelle, éliminant l’idée que les individus sont les seuls responsables.

Résumé essai 3 (chapitre 6 - Micro) : nous appliquons la théorie de la distance psychologique pour explorer les mécanismes psychologiques reliant orientations culturelles individuelles et les réponses du consommateur face à la violation de ses données personnelles. À l’aide d’une enquête en ligne adressée à un large échantillon de Français (N=452), nous confirmons nos premiers résultats et montrons que l’égalité sociale et l’égalité entre les genres sont les antécédents culturels qui influencent le plus significativement les réponses, impliquant moins de distance psychologique avec la violation de données personnelles et favorisant des réponses techniques concrètes ; tandis que d’autres orientations, comme l’indépendance, n’encouragent que la préoccupation pour la protection de ses données personnelles tout en favorisant des réponses sociales ou institutionnelles.

2. Apports de chaque essai à la thèse

Comme nous le résumons dans le Tableau 28, chaque essai contribue à notre thèse dans laquelle nous défendons qu'une préférence culturelle pour des valeurs d'égalité sociale et de genre amène les individus à être plus engagés et actifs face à des violations de leurs données personnelles. Le premier essai révèle qu'une préférence culturelle pour la féminité (e.g., les soins apportés aux autres) influence plus le comportement de plainte face à une violation de données personnelles, qu'une préférence pour l'individualisme. Le deuxième essai montre que la défense d'une égalité sociale est une motivation essentielle à l'adoption d'une réponse active face aux violations de données personnelles. Enfin, le troisième essai expose le fait que l'égalité sociale et l'égalité entre les genres sont les antécédents culturels qui influencent le plus significativement les réponses, et souligne, en outre, le rôle central de la distance psychologique avec les violations de données personnelles dans les mécanismes reliant les orientations culturelles aux réponses.

Tableau 28 : Apports de chaque essai à la thèse

	Essai 1 : Macro	Essai 2 : Méso	Essai 3 : Micro
	Influence de la culture nationale	Influence des normes socio-culturelles	Influence des orientations culturelles individuelles
Principaux résultats	- Influence positive de la féminité, de l'individualisme et de la tradition sur le comportement de plainte face à une violation de ses données personnelles - La préférence pour la féminité (souci de la communauté) et à la tradition sont plus importants que la préférence pour l'individualisme	- Montre que la défense d'une égalité sociale est une motivation essentielle à l'adoption d'une réponse active face aux violations de données personnelles - Envisage la question de la protection de la vie privée comme une pratique sociale	- Influence plus significative de l'égalité sociale et l'égalité entre les genres sur les réponses, que l'indépendance - L'égalité socio-genrée implique moins de distance psychologique avec la violation de données et favorise des réponses techniques - L'indépendance n'encourage que la préoccupation pour la protection des données personnelles
Contributions de l'essai à la thèse	- Met en avant l'importance d'une préférence pour la féminité par rapport à l'individualisme dans le comportement de plainte face à une violation de ses données personnelles	- Confirme l'importance d'une égalité sociale - Envisage la protection de la vie privée comme une pratique sociale, et non individuelle - Apporte une vision plus approfondie et novatrice des schémas motivationnels pour répondre face à une violation de données personnelles	- Confirme l'importance d'une préférence culturelle pour l'égalité socio-genrée - Confirme le rôle essentiel de la distance psychologique avec les violations de données personnelles - Minore l'importance de la préoccupation pour la protection de ses données personnelles

3. Contributions des auteurs et stade d'avancement dans la publication des essais

Chronologiquement les essais ont été conduits dans l'ordre suivant : macro (à partir d'octobre 2019 avec un enrichissement annuel de la base de données), micro (à partir de janvier 2021) et méso (à partir d'octobre 2021). Au fur et à mesure, l'autrice a pris en autonomie, diminuant ainsi le rôle des directrices de recherche dans la réalisation des essais. L'essai méso a été réalisé de manière indépendante (cf. Tableau 29).

Les essais macro et micro ont été présentés à plusieurs conférences avec comité de lecture (cf. biographie de chaque essai au début de chaque chapitre). Ils sont actuellement en cours d'écriture pour soumission à un journal. L'essai méso sera présenté en mai 2023 au congrès de l'afm (Association Française du Marketing).

Tableau 29 : Contributions des auteurs et état d'avancement de chaque publication

	Essai 1 : Macro	Essai 2 : Méso	Essai 3 : Micro
	Influence de la culture nationale	Influence des normes socio-culturelles	Influence des orientations culturelles individuelles
Contributions des autrices	Cet essai est un travail conjoint avec les directrices de recherche. Les coautrices ont analysé les données et rédigé ensemble cette première communication. L'autrice s'est chargée de la revue de la littérature.	Cet essai est un travail indépendant	Cet essai est un travail conjoint avec les directrices de recherche. Les coauteurs ont analysé ensemble les résultats. L'autrice a réalisé l'essentiel du travail pour ce chapitre (e.g., littérature, design de la recherche, questionnaire, collecte, rédaction)
Stade d'évolution	Accepté à plusieurs conférences avec comité de lecture En cours d'écriture pour soumission à un journal	Accepté pour présentation au congrès de l'afm 2023	Accepté à plusieurs conférences avec comité de lecture En cours d'écriture pour soumission à un journal

Synthèse du chapitre 3 sur le cadre général de la thèse

Notre recherche consiste à explorer l'influence des valeurs culturelles sur le comportement de réponses (technique, sociale, institutionnelle) face à une violation de données personnelles. Les valeurs culturelles sont observées à trois niveaux (macro, micro et méso) et chaque niveau d'observation correspond à un essai.

Le premier essai (macro) éclaire l'influence de la culture nationale sur le comportement de plainte pour violation de ses données personnelles. Le deuxième essai (méso) observe l'influence des normes socio-culturelles sur le comportement de réponse face à une violation de ses données, tout en analysant les mécanismes sociologiques et les schémas motivationnels amenant à une réponse. Le troisième essai (micro) vise à comprendre l'influence des orientations culturelles individuelles et les mécanismes psychologiques reliant valeurs culturelles et réponse.

Enfin chaque essai, avec différents angles épistémologiques, contribue à enrichir notre compréhension de l'importance d'une préférence culturelle pour une égalité sociale dans les comportements de réponse face à une violation de données personnelles.

Nos trois essais correspondent aux trois chapitres suivants.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

Protection
des données
personnelles

Réponses des
consommateurs
insatisfaits

Culture
et valeurs



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :

Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :

Influence des
normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :

Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 4. Essai 1 - Influence de la culture nationale sur le comportement de plainte pour violation de données personnelles



Résumé de l'essai

L'Europe a adopté en mai 2018 le RGPD afin de renforcer la protection des données personnelles des citoyens, notamment en leur permettant de déposer une plainte en cas de violation de données personnelles auprès des autorités nationales pour la protection des données personnelles (e.g., CNIL en France). Constatant une grande variance dans le nombre de ces plaintes, cette recherche examine l'influence de la culture nationale sur le comportement de plainte pour violation des données personnelles. Nous mobilisons une base de données recensant les plaintes déposées pour violation de données personnelles auprès des autorités nationales (e.g., CNIL en France), base de données enrichie des dimensions culturelles d'Hofstede (Hofstede, 1984, 2001; Hofstede et al., 2010). Nous observons que les individus issus de pays européens valorisant davantage la féminité (i.e., l'égalité des sexes et les soins communautaires) ont tendance à se plaindre davantage, de même, mais dans une moindre mesure, que ceux issus de pays européens valorisant davantage l'individualisme (i.e., une préférence pour l'autonomie, l'indépendance et la liberté individuelle, privilégiées au collectivisme et à la défense du groupe social) ou la tradition. Cette recherche regroupe les pays européens en trois ensembles, pour lesquels les moyens d'adoption et d'application du RGPD pourraient être adaptés. Nous discutons ces perspectives.

Biographie de cet article

Une communication extraite de ce chapitre a été présentée à la 10^{ème} conférence Atlas-AFMI (18-20 mai 2020 ; IAE de Poitiers, France) et à la conférence régionale 2020 de l'EMAC, European Marketing Academy (16-19 septembre 2020 ; Zagreb, Croatie).

Section 1. Introduction et fondements de la recherche

1. Introduction

Entre mai 2018 et janvier 2022, les autorités administratives pour la protection des données personnelles ont enregistré aux Pays Bas 300.7 plaintes pour 100.000 personnes pour violation de données personnelles, contre 286.2 au Danemark, 129.4 en Allemagne, 24.2 en Belgique, 9.7 en France, 5.4 en Italie⁸⁵, soit un rapport de 1 à 31 entre la France et les Pays-Bas. Ces plaintes pour violations de données personnelles sont notifiées aux autorités pour la protection des données personnelles de chaque pays (e.g., CNIL, en France ; cf. liste des autorités européennes en Annexe 3) dans le cadre du RGPD entré en vigueur en mai 2018. Le RGPD a pour objectif de renforcer les droits des utilisateurs, tout en harmonisant les réglementations précédentes au sein de l'Europe. Dans cette perspective, les autorités nationales, qui supervisent l'application du RGPD, remplissent une mission importante en informant, en contrôlant l'application du RGPD, et en instruisant les réclamations. Dans le cas de non-respect du RGPD par une organisation⁸⁶, elles peuvent aussi imposer aux entreprises des pénalités pouvant atteindre 20 millions d'euros ou 4% de leur chiffre d'affaires annuel mondial : l'Irlande, la France et l'Italie ont à ce titre imposé des amendes très importantes (e.g., 225 millions d'euros par l'autorité irlandaise à WhatsApp en septembre 2021 ou 150 millions d'euros en France à Google en janvier 2022⁸⁷). Ces sanctions sont souvent prononcées par les autorités administratives nationales suite à des actions collectives telles que celles de « My Privacy is None of Your Business », organisation de l'Autrichien Maximillian Schrems, qui a émis 101 plaintes auprès de différentes autorités, ou la Quadrature du Net en France.

Si ces amendes sont en très forte progression, à l'inverse le nombre de plaintes déposées par des citoyens aux régulateurs de la protection des données personnelles se stabilise dans le temps après avoir connu une très forte progression en 2018 (avec une moyenne de 356 notifications pour violations de données par jour en Europe entre janvier 2021 et janvier 2022 , soit une

⁸⁵ DLA Piper GDPR fines and data breach survey. *op. cit.*

⁸⁶ Le RGPD oblige toute organisation qui collecte des données à enregistrer les processus de collecte de données, sous la responsabilité d'un délégué à la protection des données, et à alerter les individus dans les 72 heures en cas de violation de données personnelles

⁸⁷ cf. <https://www.enforcementtracker.com>

progression de seulement +8% par rapport à l'année précédente⁸⁸) et entre chaque pays (le classement des pays selon le nombre de plaintes pour 100.000 habitants varie peu depuis 2018), traduisant une situation devenue structurelle et non un épiphénomène conjoncturel lié à l'entrée en vigueur du RGPD. De plus, les plaintes sont essentiellement le fruit d'actions individuelles. En France, les motifs restent surtout liés à la prospection commerciale intrusive et à la surveillance au travail (source CNIL – LINC 2021⁸⁹).

Cette variabilité entre pays européens tant dans le nombre de plaintes déposées aux autorités que dans les montants des sanctions qu'elles appliquent peut s'expliquer par des effets culturels propres à chaque pays, comme le rapport à la loi, la confiance institutionnelle, le sens des responsabilités individuelles, la perception de la plainte, le souci de protection de sa vie privée, le rapport au risque, à la sécurité ou à la vulnérabilité. **Par conséquent, nous nous interrogeons sur le rôle de la culture dans le comportement de plaintes pour violation de la protection des données personnelles.**

Jusqu'alors, les chercheurs (e.g., Smith et al., 2011) se sont intéressés aux antécédents (individuels, contextuels et culturels) à l'*information privacy concern*, i.e., la préoccupation concernant la manière dont les données personnelles sont collectées et utilisées par des tiers (Belanger et al., 2002). Les recherches mettent en exergue l'effet indéniable de la culture sur cette préoccupation pour la protection de la vie privée (e.g., Miltgen & Peyrat-Guillard, 2014). Elles se sont essentiellement concentrées sur le lien entre une préférence culturelle pour l'individualisme (i.e., une préférence pour l'autonomie, l'indépendance et la liberté individuelle ; Hofstede, 1984) et le souci de protection de la vie privée (e.g., Dinev et al., 2006 ; James et al., 2017 ; Krasnova et al., 2012 ; Steenkamp & Geyskens, 2006). Cependant, des résultats contradictoires apparaissent (e.g., Lowry et al., 2011), et appellent à davantage de recherches (e.g., Martin et al., 2020), notamment à explorer un spectre plus large de dimensions culturelles : élargir les réflexions au-delà de l'idée qu'une préférence pour l'individualisme conduit à des comportements plus protecteurs de la vie privée paraît encourageant.

De plus, étudier les effets culturels au regard d'un comportement nouveau, i.e., le comportement de réponses face aux violations de données personnelles, pourrait faire apparaître des résultats prometteurs. En outre, cela favoriserait la compréhension du comportement de réponse et de

⁸⁸ La CNIL a reçu 14.143 plaintes en 2021 soit + 4% vs 2020 (cf. rapport d'activités CNIL 2021. *op. cit.*)

⁸⁹ <https://linc.cnil.fr/fr/la-protection-des-donnees-est-elle-un-sport-de-riches>

plainte face à une violation de données personnelles, qui a jusqu'alors très peu été explorée, et d'identifier des pistes d'actions nécessaires au regard de la prolifération des violations de données personnelles.

En effet, les réponses des consommateurs à une violation de leurs données personnelles ont très peu été étudiées (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018). Son & Kim (2008) ont établi une taxonomie des comportements pour la protection de la vie privée, qui peut être enrichie. Romanosky et al. (2013) ont exploré le processus des poursuites pour violation de données, depuis la plainte jusqu'au règlement. Ils indiquent que seulement 3,7 % d'un échantillon de violations de données américaines signalées entre 2000 et 2010 ont fait l'objet d'un procès devant un tribunal fédéral. La probabilité d'un procès augmente proportionnellement au nombre de données perdues et à leur sensibilité (e.g., données bancaires), à la présence d'un préjudice réel démontrable, et au type de violations (e.g., piratage informatique, perte de matériel). Cependant, cette recherche porte sur les procédures de plaintes pour violation de la protection des données personnelles (afin d'identifier les caractéristiques des plaintes déposées et des procédures instruites) et non sur les manifestations comportementales de plainte face à une violation de la vie privée. Plus récemment, Labrecque (2021) évalue l'impact du stress et du sentiment de violation de contrat social générés par une violation de données personnelles sur les réponses des consommateurs : elle montre que ces réponses diffèrent selon le degré de sensibilité de données et la possibilité de rompre toute relation avec l'entreprise responsable de la violation de données. Mais cette recherche ne précise pas spécifiquement le comportement de plainte. Et, aucune des recherches citées n'aborde le rôle d'antécédents culturels : notre recherche vise à comprendre ce phénomène.

Pour ce faire, nous mobilisons le modèle de culture nationale d'Hofstede (Hofstede, 1984, 2001; Hofstede & Minkov, 2010) ainsi que les précédentes recherches portant sur l'influence de la culture sur la préoccupation pour la protection des données personnelles. À l'aide d'une base de données, regroupant les valeurs des dimensions culturelles d'Hofstede (<https://www.hofstede-insights.com>) et les données du nombre de plaintes en libre accès issus des enquêtes annuelles du cabinet DLA Piper (2019, 2020, 2021, 2022) pour 4 années et 27 pays européens⁹⁰, nous observons que les individus issus de pays européens valorisant davantage la féminité (i.e., l'égalité des sexes et les soins communautaires) ont tendance à se plaindre davantage, mais dans une moindre mesure que ceux issus de pays européens valorisant davantage l'individualisme

⁹⁰ DLA Piper GDPR fines and data breach survey. *op. cit.*

(i.e., une préférence pour l'autonomie, l'indépendance et la liberté individuelle, privilégiées au collectivisme et à la défense du groupe social) ou la tradition. Cette recherche regroupe les pays européens en trois ensembles, pour lesquels les moyens d'adoption et d'application du RGPD pourraient être adaptés.

2. Fondements théoriques

Dans cette partie, afin d'éviter toute répétition avec des éléments conceptuels précédemment énoncés dans les chapitres précédents (essentiellement chapitres 1 et 2), nous indiquons uniquement les points essentiels des fondements théoriques de notre recherche et nous indiquons les paragraphes à consulter pour des développements plus complets.

2.1. Souci de contrôle de ses données personnelles et « contrat social »

La préoccupation pour la protection de la vie privée est née à la fin du XIX^{ème} siècle avec l'émergence des médias et est devenue avec le développement des technologies un enjeu majeur de nos sociétés (Beke et al., 2018). Elle repose principalement sur le souci de contrôle de ses données personnelles (*information privacy concern*).

Nous renvoyons au chapitre 2 (section 1 – des pages 87 à 100) afin de consulter les différentes conceptualisations et constructions du souci de contrôle de ses données personnelles.

Dans le cadre de cet essai, il est intéressant de réaffirmer le rôle de la confiance et de la transparence, et donc du « contrat social » que ces dimensions constituent, lorsque des consommateurs sont amenés à prendre des décisions en matière de protection de leur vie privée (e.g., divulguer leurs données personnelles). En effet, ces décisions sont influencées par des facteurs facilitateurs, essentiellement le contrôle et la transparence dans l'échange de ses données, et inhibiteurs comme le risque perçu (Dinev & Hart, 2006; Dinev et al., 2006). La perception des dimensions de confiance et de transparence dépend des contextes culturels et des « contrats sociaux » des sociétés dans lesquelles l'observation est faite.

- D'une part, le contrôle repose sur le contrôle de l'accès à soi-même (Altman, 1975), le contrôle de ses limites personnelles et de ses contacts avec les autres (Pedersen, 1997), la réclamation des individus, des groupes, des institutions pour déterminer quand, comment et dans quelle mesure les informations personnelles sont communiquées aux autres (Westin, 1967). Les réglementations mises en place offrent à chacun le droit de contrôler la divulgation de ses informations (e.g., à travers l'obligation de consentement). Or, nous n'avons pas toujours le contrôle parfait de nos données.
- C'est pourquoi une transparence dans l'échange est nécessaire, qui repose sur l'existence d'un « contrat social », i.e., des attentes conventionnelles et implicites entre personnes et/ou organisations, reposant sur des normes généralement comprises, selon lesquelles les informations personnelles partagées et/ou utilisées sont protégées (Donaldson & Dunfee, 1994; Dunfee et al., 1999). La théorie du contrat social suggère que la transparence garantit un échange équitable d'informations entre les consommateurs et les organisations (Culnan & Bies, 2003) et les consommateurs tiennent compte de la transparence dont les organisations font preuve dans les échanges. Le contrat social est basé sur un consentement éclairé soutenu par un droit de sortie.

La transparence diminue la perception de violation de vie privée (Martin et al., 2017), rend les consommateurs plus disposés à divulguer des informations (Son et Kim, 2008). De plus, les consommateurs sont plus susceptibles de croire que les entreprises ont rempli leur part du « contrat social » lorsqu'ils perçoivent une personnalisation de l'échange (Chellappa & Sin, 2005), ou un dédommagement financier (Gabisch & Milne, 2014).

Enfin, le contrôle de l'accès à ses données personnelles et la transparence dans l'échange et l'usage de données personnelles renforcent la confiance entre les acteurs. La confiance prend un rôle central dans la relation d'échange. Le « contrat social » devient un « contrat de confiance ».

Ce rôle de la confiance dans les échanges de données personnelles intervient dans un contexte général de confiance institutionnelle et de confiance dans les technologies (Lippert & Swiercz, 2005), qui peut varier selon des variables culturelles. Dinev et al. (2006) utilisent le cadre de la confiance et du capital social de Fukuyama (1995) en parallèle des dimensions d'Hofstede pour expliquer les différences de préoccupations pour la protection des données personnelles entre les États-Unis et l'Italie. Selon la théorie de la confiance (Fukuyama, 1995), il existe une

corrélation entre la prospérité économique d'un pays et son niveau de capital social. Le capital social correspond aux caractéristiques d'une organisation sociale, telles que la confiance et la fiabilité, qui permettent à des entreprises de se développer au-delà d'un cadre traditionnel et familial et d'améliorer leur efficacité en développant des collaborations fondées sur la confiance. Fukuyama identifie des pays « à forte confiance » (e.g., États-Unis, Allemagne, Japon) et de pays « à faible confiance » (e.g., Italie, France). Ces résultats sont confirmés par une étude réalisée par ourworldindata.org indiquant que 19% des Français déclarent en 2009 qu'« il est possible de faire confiance à la plupart des gens » contre 30% des personnes interrogées au Royaume-Uni et 68% en Suède ⁹¹.

Les notions de transparence et de confiance sont liées. Les pays à forte confiance (Fukuyama, 1995) vont favoriser la transparence dans les affaires (e.g., transparence fiscale, transparence des mesures de vigilance climatique) et les relations sociales (e.g. la Norvège). La transparence institutionnelle peut, de ce fait, développer la compréhension des règles de contrat social sur lesquels repose la protection des données personnelles. Enfin, ces différents degrés de confiance et de transparence impactent également l'acceptation de toute rupture de ce contrat ou de non-respect d'un engagement contractuel implicite (Dunfee et al., 1999).

2.2. Comportement de plainte individuelle

Face au non-respect des engagements contractuels de l'entreprise de protection de la vie privée et des données personnelles, l'individu peut exprimer son mécontentement de différentes manières (Son & Kim, 2008) selon trois options : *loyalty*, *exit* ou *voice* (Hirschman, 1970). Si cette trichotomie ancienne nécessite d'être actualisée dans un contexte de digitalisation des services, de possibilités de responsabilisation et de moyens de plainte plus importants grâce à Internet et aux réseaux sociaux (Jasper & Waldhart, 2013; N'Goala et al., 2019), elle offre une bonne compréhension des motivations de plainte, que nous montrons ci-dessous.

La *loyalty* est l'absence d'alternative abordable, i.e., la résignation, le refus de l'idée de faire changer les choses. Dans le cas contraire et dans un objectif de faire changer les choses face à la défaillance d'une entreprise (e.g., baisse de la qualité des produits et des services), le consommateur a deux alternatives : la défection (*exit*) ou la prise de parole (*voice*). Le titre de

⁹¹ <https://ourworldindata.org/trust>

l'ouvrage « Exit, Voice and Loyalty » d'Hirschman (1970) est d'ailleurs traduit en français par « Défection et prise de parole ». La défection relève de l'économie, car elle fait le jeu de la concurrence du marché : le marché offre des possibilités de choix et la correction des défaillances se manifeste pour un changement d'offre, selon la règle de la « main invisible » d'Adam Smith. La défection n'est pas toujours possible quand il n'existe pas ou peu de concurrence, comme dans le cas des institutions publiques, des entreprises en quasi-monopole (ex. SNCF) ou des biens durables (ex. automobile). Finalement, la défection est relativement bien encadrée par les lois anticoncurrentielles. À l'opposé, la prise de parole, qui va « du ronchonnement à peine perceptible à la récrimination violente » (Hirschman, 1970, p.27), est une prise de position directe et relève du politique. La *voice* est l'expression d'un manque d'alternative et du sentiment d'être pris au piège. En somme, la prise de parole est « l'action politique par excellence » (p.27), en rapport direct avec le cadre concurrentiel et institutionnel dans lequel il s'exprime. Or, la prise de parole est moins encadrée par la loi et le droit d'interpellation des citoyens-usagers n'est pas toujours reconnu au niveau du droit de la concurrence comme mécanisme de correction de l'économie.

En dernier lieu, le choix entre défection et prise de parole est influencé par le contexte culturel et le niveau socio-éducatif. Par exemple, selon Hirschman, les Américains ne seraient pas amenés à exprimer leur mécontentement, car ils ont historiquement la possibilité et l'habitude de quitter ce qui ne leur plaît pas (phénomène de fuite) plutôt que d'exprimer leur mécontentement et de se battre pour leurs droits. Nous allons alors préciser le modèle d'Hofstede de mesure à un niveau national des effets culturels.

2.3. Modèle de la culture nationale d'Hofstede

Définie comme « l'ensemble complexe qui comprend les connaissances, les croyances, l'art, la morale, les coutumes et toutes les autres capacités et habitudes acquises par l'homme en tant que membre de la société » (Tylor, 1871, p.97, cité par McCort & Malhotra, 1993), la culture a été opérationnalisée par l'utilisation de proxys tels que le partage d'un système de croyances et de valeurs spécifiques (Lenartowicz & Roth, 1999). Considérant que « la culture est un concept trop global pour être significatif en tant que variable explicative [...] et devrait être remplacée par ses constituants » (Van de Vijver et al., 1997, p.3), cette approche vise à identifier des dimensions fiables pour résumer les aspects les plus pertinents de la culture. Le modèle de la

culture nationale de Hofstede (Hofstede, 1984, 1991, 2001; Hofstede et al., 2010) est le plus connu et utilisé.

Nous renvoyons au chapitre 1 (section 2 – pages 68 à 69) et au chapitre 2 (section 3 – page 141) pour une présentation détaillée du modèle d'Hofstede.

L'utilisation du modèle de la culture nationale d'Hofstede dans le cadre de cet essai nous semble pertinente. D'une part, les dimensions d'Hofstede présentent l'avantage de pouvoir analyser simplement le lien entre nos différents concepts, qui seront ensuite explorés plus précisément dans le cadre de notre recherche doctorale. D'autre part, nous mobilisons les dimensions à un niveau d'analyse macro et nationale (et non individuelle), avec pour objectif de décrire de manière simple les différences nationales en matière de plainte pour violation de la protection des données personnelles.

3. Étude exploratoire de la culture nationale en Europe

Nous proposons de commencer par une observation exploratoire de la manière dont la culture nationale est structurée en Europe (considérant que le contexte européen a été relativement peu exploré jusqu'à présent dans le cas de la préoccupation pour la vie privée ; Miltgen & Peyrat-Guillard, 2014; Posey et al., 2010). Pour ce faire, nous rassemblons d'abord les mesures des 6 dimensions de la culture nationale pour les pays européens telles que fournies par Hofstede pour 27 des 28 pays européens sur son site web <https://www.hofstede-insights.com/> (les données chypriotes sont manquantes). Le détail des scores par pays est présent en Annexe 7.

Nous effectuons ensuite une analyse factorielle sur ces six dimensions.

Tableau 30 : Statistiques descriptives et corrélations des dimensions d'Hofstede sur 27 pays européens

	Distance hiérarchique	Individualisme	Masculinité	Contrôle de l'incertitude	Orientation à long terme	Indulgence
Mean	51.44	58.63	46	70.59	57.52	43.44
Std dev.	20.83	17.84	24.57	21.99	16.66	19.69
Min	11	27	5	23	24	13
Max	100	89	100	100	83	78
Distance hiérarchique	1	-.564**	.192	.584**	.131	-.507**
Individualisme		1	.114	-.561**	.169	.391*
Masculinité			1	.155	.080	-.072
Contrôle de l'incertitude				1	.032	-.406*
Orientation à long terme					1	-.407*

* $p < .05$, ** $p < .01$

Comme indiqué dans le Tableau 30 et déjà relevé par la littérature (e.g., Pelau et Pop, 2018), les dimensions de distance hiérarchique, individualisme et contrôle de l'incertitude apparaissent fortement corrélés ($\rho > .50$, $p < .01$). En outre, l'indulgence, la sixième dimension, est corrélée avec quatre des cinq autres dimensions du modèle de Hofstede ($.39 < \rho < .51$, $p < .05$). Nous l'excluons donc et réalisons une analyse factorielle en utilisant uniquement les 5 dimensions originales : cette analyse ne révèle que 3 facteurs principaux (voir Tableau 31). Ces résultats sont cohérents avec des recherches antérieures (e.g., Bellman et al., 2004; Minkov, 2018) soulignant que dans un contexte européen certaines des dimensions de Hofstede sont fortement corrélées, y compris Hofstede lui-même (2001).

Tableau 31 : Analyse factorielle des dimensions d'Hofstede sur 27 pays européens

	Facteur 1 Individualisme	Facteur 2 Masculinité	Facteur 3 Orientation long terme
Individualisme	.795		
Distance hiérarchique	-.907		
Contrôle de l'incertitude	-.904		
Masculinité		.986	
Orientation à long terme			.984

Dans la suite de notre recherche, nous considérons les 3 facteurs principaux comme les 3 dimensions pertinentes de la culture nationale en Europe :

- Le premier facteur fortement corrélé avec *individualisme*, *contrôle de l'incertitude* (inverse) et *distance hiérarchique* (inverse) est nommé « **individualisme** ». Ainsi, les pays européens valorisant le plus l'individualisme présentent les caractéristiques suivantes : ils favorisent l'autonomie, les choix, la définition des objectifs et l'orientation individuelle. Dans ces pays, la distance hiérarchique est faible, ce qui signifie que les membres les moins puissants des organisations et des institutions (comme la famille) acceptent moins une distribution inégale du pouvoir et considèrent que chacun est responsable et doit défendre ses droits. De même, la tolérance à l'incertitude et à l'ambiguïté est élevée et les règles établies sont moins nécessaires pour gérer cette incertitude. Dans notre recherche, les pays les plus individualistes sont le Danemark, le Royaume-Uni et la Suède ;
- Le second facteur est celui de la « **masculinité** ». Dans notre recherche, les pays les plus masculins sont la Hongrie, l'Autriche et l'Italie ;
- Le troisième facteur représente l'« **orientation à long terme** ». Dans notre recherche, les pays valorisant le plus l'orientation à long terme sont la Belgique, la Lituanie et l'Allemagne.

Section 2. Modèle conceptuel et hypothèses de recherche

Après avoir détaillé nos fondements théoriques, nous étayons dans cette section nos différentes hypothèses de recherche.

1. Individualisme et plainte pour protection des données personnelles

Dans les pays qui valorisent l'individualisme, les personnes pensent probablement que chacun a le droit de défendre sa vie privée (Milberg et al., 2000). Les personnes individualistes sont plus susceptibles de réclamer des dommages aux entreprises ou d'exprimer leur mécontentement aux autres (Chapa et al., 2014; Liu et al., 2001; Liu & McClure, 2001). Nous nous attendons à ce que ces personnes n'acceptent pas de traitement inégal et d'incidents tels que des violations de données, en raison d'une distance hiérarchique plus faible. Elles sont susceptibles de se sentir plus responsables, n'attendant pas tout de ceux qui ont une charge de responsabilités (Girerd-Potin et al., 2018). Il en résulte que ces personnes se sentent individuellement responsables du maintien d'un certain ordre social et n'attendent pas que les autorités administratives nationales remplissent leur mission, par exemple en imposant des sanctions financières. En outre, en raison d'un plus faible contrôle de l'incertitude, il est probable qu'elles expriment plus facilement une plainte car elles sont à l'aise et moins stressées dans des situations ambiguës, donc susceptibles de prendre des risques pour exprimer leur plainte. En effet, se plaindre est souvent perçu comme un comportement risqué qui implique de faire face à l'incertitude de la résistance de l'entreprise visée par la plainte et au caractère indésirable d'un conflit ouvert. À l'inverse, les personnes issues de cultures à faible contrôle de l'incertitude acceptent plus volontiers les risques (Huang et al., 1996). Les personnes issues de pays valorisant l'individualisme portent donc plus facilement plainte pour défendre leurs droits en général et leur vie privée en particulier.

Par ailleurs, nous supposons que les personnes individualistes sont plus susceptibles de comprendre les normes implicites de contrôle, transparence et confiance sur lesquelles se fondent le contrat social (Donaldson & Dunfee, 1994; Dunfee et al., 1999) régissant l'usage et le partage des données personnelles. En effet, individualisme, confiance et prospérité économique sont liés. Il est démontré que le PIB d'un pays est fortement corrélé avec les dimensions culturelles nationales telles que la distance au pouvoir ou l'individualisme (e.g.,

Hofstede, 2001 ; Gorodnichenko & Roland, 2011). Et la prospérité économique d'un pays influe sur son niveau de capital social et sur la confiance sociale (Fukuyama, 1995). De plus, une culture individualiste prédispose l'individu à faire plus facilement confiance à une personne appartenant à « l'out-group », i.e., en dehors de son cercle de proches (famille, amis, collègues) (Huff & Kelley, 2003). Les personnes individualistes sont plus susceptibles de se plaindre car elles perçoivent la violation des normes sociales engendrée par une violation de leurs données personnelles et atteinte à leur vie privée.

Enfin, les personnes individualistes sont d'autant plus susceptibles d'exprimer une parole politique de plainte (Hirschman, 1970) que le niveau de confiance institutionnelle est élevé dans leur pays. S'il peut être moins probable d'être sceptique sur la violation de la vie privée, il est plus probable de se plaindre si cette violation se produit réellement, car les institutions sont censées agir de manière décente et efficace. Dans un pays individualiste, la loi, plus que la communauté, est là pour défendre les droits et l'individu.

Dans l'ensemble, nous supposons que, dans les pays européens qui valorisent l'individualisme (e.g., le Danemark, le Royaume-Uni et la Suède), les individus ont tendance à se plaindre davantage pour la violation de leurs données personnelles.

H1 : Une préférence culturelle nationale pour l'individualisme a une influence positive sur le comportement de plainte des individus pour violation des données personnelles.

2. Masculinité et plainte pour protection des données personnelles

Dans l'ensemble, nous supposons que dans les pays européens qui valorisent la masculinité (e.g., la Hongrie, l'Autriche et l'Italie), les individus ont tendance à moins se plaindre dans le cas de violation de données personnelles, pour trois raisons.

Tout d'abord, les individus issus de pays valorisant la masculinité mettent davantage l'accent sur la réussite et l'accomplissement, et se préoccupent moins de la défense et du bien-être de la communauté que les pays à orientation féminine (comme la Suède ou la Norvège). Par conséquent, ils s'intéressent moins à la protection de la vie privée et familiale, conformément

au fait que la masculinité a déjà été corrélée négativement avec la préoccupation pour la vie privée (Bellman et al., 2004).

De plus, et alors même que la défense de la vie privée oscille entre défense des droits fondamentaux et défense des intérêts économiques d'acteurs privés (Rochelandet, 2010), il est probable que dans les cultures valorisant la masculinité, les individus vont être intéressés par la réussite et les gains économiques. Ils prennent moins le temps de faire changer les choses et sont plus à la recherche d'alternatives économiques. Les individus valorisant la masculinité sont plus orientés vers l'action, pragmatiques et sont moins normatifs : ils sont donc peu susceptibles de prendre le temps de se plaindre et de définir des règles.

Finalement, la confiance institutionnelle est moins importante dans les pays à orientation masculine (e.g., Italie) (Dinev et al., 2006) : la plainte individuelle et pragmatique semble moins probable, car peu utile compte tenu du fait que les institutions sont perçues comme peu efficaces.

H2 : Une préférence culturelle nationale pour la masculinité a une influence négative sur le comportement de plainte des individus pour violation des données personnelles.

3. Orientation à long terme et plainte pour protection des données personnelles

Dans les pays qui valorisent l'orientation à long terme, la préparation de l'avenir est importante et gérée comme un équilibre entre des situations parfois contradictoires, et pour lequel la plainte n'est pas efficace ou n'est pas forcément la solution pour préparer l'avenir. Dans les sociétés orientées vers le court terme, les traditions et les normes sociales sont au premier plan. Dans un contexte professionnel, elles sont considérées comme normatives. Le futur est parfois regardé avec suspicion, et des règles, éventuellement établies à la suite de plainte, sont établies pour préparer l'avenir. À l'inverse dans les pays à orientation long terme, l'approche est plus pragmatique, regardant les coûts et les bénéfices de tout changement. De la même manière, les institutions se construisent dans une recherche de compromis (par exemple, les syndicats en Allemagne ont un rôle de construction collaborative avec les employeurs et non d'opposition à

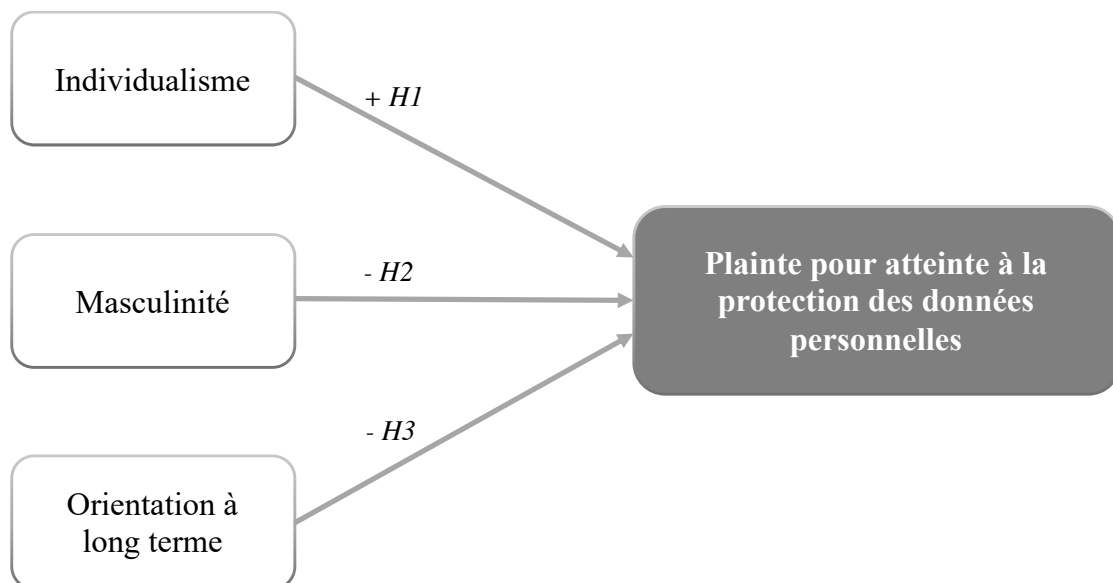
tout changement), où l'institutionnalisation est la responsabilité de chacun. En outre, les personnes valorisant l'orientation à long terme sont plus tolérantes et plus calmes (Mariani et al., 2019) et devraient donc se plaindre moins souvent en cas de violation de la protection des données personnelles.

Nous supposons que dans les pays européens qui valorisent l'orientation à long terme (e.g., Belgique, Lituanie et Allemagne), les individus ont tendance à moins se plaindre pour la violation de leurs données personnelles.

H3 : Une préférence culturelle nationale pour l'orientation à long terme a une influence négative sur le comportement de plainte des individus pour violation des données personnelles.

Le cadre conceptuel et les hypothèses sont récapitulés dans la Figure 25.

Figure 25 : Cadre conceptuel de l'essai 1 portant sur l'influence de la culture nationale



Section 3. Recherche empirique et résultats

1. Méthodologie

Pour tester nos hypothèses, nous avons complété la base de données utilisée dans notre étude exploratoire. Concrètement, nous avons collecté le nombre de plaintes pour violation de données personnelles pour 100.000 personnes qui ont été notifiées aux autorités nationales dans le cadre du RGPD pour 4 périodes détaillées ci-dessous, et telles qu'elles ont été rapportées par le cabinet d'avocat international DLA Piper chaque année depuis janvier 2019⁹². À noter que DLA Piper communique le nombre de plaintes pour 25 pays européens, les données de tous les pays n'étant pas disponibles chaque année (cf. dans le Tableau 32). Nous ajoutons également que les tendances restent les mêmes sur l'année 2022 (cf. rapport DLA Piper 2023).

Le Tableau 32 présente ces données. Pour tester les hypothèses, nous avons conduit une régression linéaire en deux étapes.

⁹² DLA Piper GDPR fines and data breach survey. *op. cit.*

Tableau 32 : Nombre de plaintes et dimensions culturelles pour 25 pays européens

	Nombre de plaintes pour violation de données notifiées pour 100 000 personnes				Factor 1 – Individua lisme	Factor 2 – Masculin ité	Facteur 3 – Orientatio n à long terme
	P1 du 25 mai 2018 au 28 janvier 2019 22 pays	P2 du 28 janvier 2019 au 27 janvier 2020 23 pays	P3 du 25 mai 2018 au 27 janvier 2021 23 pays	P4 du 28 janvier 2021 au 27 janvier 2022 23 pays			
Allemagne	15,60	31,12	50,00	79,42	0,471	0,786	1,377
Autriche	6,60	12,10	9,80	9,60	0,760	1,350	-0,201
Belgique	3,60	7,88	9,80	14,37	-0,552	0,648	1,810
Croatie	nd	nd	2,70	2,48	-1,229	-0,492	-0,089
République tchèque	2,70	4,03	2,90	2,25	-0,309	0,417	0,743
Danemark	53,30	115,43	155,60	130,60	1,838	-1,199	-1,318
Estonie	-	9,74	11,20	14,97	0,283	-0,754	1,341
Finlande	45,10	71,11	71,80	85,59	0,655	-0,650	-1,053
France	1,90	3,20	2,80	6,88	-0,500	0,175	0,722
Grèce	0,60	1,50	1,30	1,45	-1,204	0,487	-0,786
Hongrie	2,70	4,87	8,50	13,53	0,287	2,070	0,282
Irlande	74,90	132,52	127,80	130,19	1,417	0,904	-2,023
Italie	0,90	2,05	2,50	2,86	0,219	1,228	0,431
Lettonie	2,80	6,13	5,40	4,89	0,360	-1,350	0,882
Lituanie	nd	4,18	7,00	13,97	0,139	-1,134	1,417
Luxembourg	33,00	56,97	59,60	57,76	0,184	0,205	0,348
Malte	22,30	31,00	23,80	22,23	-0,594	0,378	-0,347
Pays-Bas	89,80	147,20	150,00	150,71	0,876	-1,101	0,808
Pologne	5,70	13,74	22,60	33,75	-0,735	1,031	-0,831
Portugal	1,60	nd	nd	nd	-1,376	-0,558	-1,732
Roumanie	1,20	1,90	nd	nd	-1,814	-0,368	-0,313
Slovénie	35,20	52,55	80,00	71,70	-1,436	-1,253	-0,562
Espagne	1,30	2,08	3,20	4,28	-0,601	-0,028	-0,441
Suède	24,90	48,14	48,10	54,83	1,319	-1,723	-0,233
Royaume-Uni	16,30	17,79	12,70	14,14	1,542	0,930	-0,231

2. Première étape de l'analyse

La première étape vise à régresser le nombre de plaintes pour violations des données personnelles par le PIB par habitant de chaque pays (voir équation 1 ci-dessous). L'objectif est premièrement d'exclure l'influence éventuelle de la maturité digitale dans un pays sur le nombre de plaintes pour violations de données personnelles (un plus grand degré de maturité digitale pouvant générer à la fois un plus grand risque de violations de données personnelles et une plus grande connaissance des outils de plainte) ; et deuxièmement, d'éviter les risques de multicollinéarité. De plus, il est démontré que le PIB par habitant est fortement corrélé avec les dimensions culturelles nationales telles que la distance hiérarchique ou l'individualisme (e.g., Hofstede, 2001 ; Gorodnichenko & Roland, 2011). Le PIB est, par exemple, contrôlé dans les recherches précédentes portant sur les effets culturels (e.g., Schwartz, 1992).

$$\text{(Equation 1)} \quad \text{Nombre\_Violations}_i = \alpha \cdot \text{PIB}_i + \beta + \varepsilon_i$$

où Number_Breaches_i est le nombre de plaintes notifiées pour violations de données personnelles de chaque pays i ; GNP_i est le PIB par habitant du pays i ; α est le coefficient estimé ; β est une constante ; et ε_i est le résidu obtenu pour chaque pays i .

Cette première régression ($R^2=0,266$, $F(1,20)=7,25$, $p=.014$; résultats pour la première période P1 ; les résultats pour chacune des 4 périodes sont présentés dans Tableau 33) valide que le PIB a une influence significative et positive sur le nombre de violations de la protection des données personnelles notifiées aux autorités ($\alpha = .716$, $p=.014$). Cette régression est significative pour chacune des 4 périodes de l'analyse (cf. Tableau 33).

Tableau 33 : Résultats de la première régression

	P1	P2	P3	P4
R²	0,266	0,280	0,170	0,216
ddl	F (1,20) = 7,25	F (1,21) = 8,164	F (1,20) = 5,293	F (1,20) = 5,499
p	0,14	0,009	0,032	0,029
α	0,716	1,280	1,242	1,205

Cette première étape de l'analyse nous permet d'isoler des résidus (ε_i) obtenus pour chaque pays et de créer pour chaque pays une variable représentant ces résidus. Cette dernière représente l'écart entre la valeur du nombre de plaintes observées réellement pour chaque pays ($\text{Nombre\_Violations}_i$) et la valeur prédite fonction du PIB. Plus la valeur du résidu est proche

de 0, plus la valeur réelle et la valeur prédite sont proches : le PIB a alors peu d'effet sur le nombre de plaintes. La valeur de cette variable résiduelle peut être positive ou négative selon les pays et les périodes. Si la valeur est positive, cela signifie que le nombre de plaintes observé (valeur réelle) est plus important que le nombre de plaintes fonction du PIB (valeur prédite) : il existe bien un effet de plainte en dehors de tout effet de PIB et maturité digitale.

3. Deuxième étape de l'analyse

Dans la seconde étape (voir l'équation 2), nous régressons les résidus provenant de la première régression par les facteurs mesurant l'« individualisme », la « masculinité » et l'« orientation à long terme » pour chaque pays i , selon l'analyse suivante :

$$\begin{aligned} \text{(Equation 2)} \quad \varepsilon_i = & \gamma_1 \cdot \text{Individualisme}_i + \gamma_2 \cdot \text{Masculinité}_i + \\ & \gamma_3 \cdot \text{Orientation Long terme}_i + \gamma_4 + \omega_i \end{aligned}$$

où ε_i est le terme résiduel de l'équation 1 pour le pays i ; Individualisme_i est la coordonnée du pays i sur le premier facteur résultant de l'analyse factorielle (voir Tableau 32) ; Masculinité_i est la coordonnée sur le deuxième facteur ; $\text{Orientation Long terme}_i$ est la coordonnée sur le troisième facteur ; γ_1 , γ_2 et γ_3 sont les coefficients estimés ; γ_4 est une constante et ω_i est le terme d'erreur.

Cette seconde régression est valide ($R^2=.379$, $F(3,18)=3.655$, $p=.016$; résultats pour la première période P1, les résultats pour chacune des 4 périodes sont présentés dans le Tableau 34). Les tests montrent que les trois principales dimensions de la culture nationale en Europe influencent significativement le nombre de plaintes pour violations de données personnelles notifiées aux autorités, positivement pour l'individualisme ($\gamma_1=.320$, $p=.043$), négativement pour la masculinité ($\gamma_2=-.372$, $p=.027$) et négativement pour l'orientation à long terme ($\gamma_3=-.277$, $p=.080$) corroborant à la fois H1, H2 et H3.

L'analyse est reconduite sur les 3 autres échantillons de données, sur les périodes P2, P3 et P4. En utilisant le même modèle de régression en deux étapes, les analyses affichées dans le Tableau 34 à nouveau corroborent H1, H2 et H3, confirmant la robustesse de nos résultats.

Tableau 34 : Résultats de la deuxième régression pour les 4 périodes

	P1 22 pays	P2 23 pays	P3 23 pays	P4 23 pays
R²	0,379 ** (p=0,016)	0,454 *** (p=0,004)	0,448 *** (p=0,006)	0,376 ** (p=0,017)
γ_1	0,320 ** (p=0,043)	0,304 ** (p=0,049)	0,270 * (p=0,096)	0,293 * (p=0,092)
γ_2	-0,372 ** (p=0,027)	-0,387 ** (p=0,014)	-0,404 ** (p=0,012)	-0,361 ** (p=0,027)
γ_3	-0,277 * (p=0,080)	-0,409 ** (p=0,014)	-0,390 ** (p=0,020)	-0,328 ** (p=0,049)

* p<.10, ** p<.05, *** p<.01

En conclusion, chacune de nos hypothèses est validée.

Section 4. Discussion et implications

Dans cette dernière section, nous allons préciser les contributions théoriques de notre recherche qui sont doubles : une meilleure compréhension des effets culturels (1) et l'identification d'un comportement de plainte spécifique (2). Nous expliquerons également l'implication pratique de notre recherche, vers une adaptation locale des moyens d'adoption du RGPD (3). Enfin, nous mettrons l'accent sur les limites de notre recherche (4) qui ouvrent la voie à de futures recherches. Certains points sont développés et approfondis dans le chapitre 7 final (discussion).

1. Contributions théoriques

1.1. Au-delà de la discussion « Individualisme culturel – protection de la vie privée »

Les précédentes recherches portant sur l'influence de la culture sur le souci de contrôle de ses données personnelles considèrent l'individualisme comme une dimension clé dans la compréhension des phénomènes (e.g., Miltgen & Peyrat-Guillard, 2014), tout en s'interrogeant sur des possibles effets contradictoires (e.g., Lowry et al., 2011) et sur des comportements étonnants notamment dans les pays comme l'Inde (cf. explications page 44), appelant alors à plus de recherches (Beke et al., 2018; Benamati et al., 2021; Martin & Murphy, 2017; Miltgen & Peyrat-Guillard, 2014).

Notre recherche permet d'identifier dans un contexte européen l'effet plus important de deux autres dimensions : la masculinité et l'orientation à long terme. À notre connaissance, l'influence de la masculinité n'avait été identifiée que par Milberg et al. (2000), et l'orientation à long terme n'avait été mobilisée que par Li et al. (2017), dans le contexte particulier d'une analyse prédictive du souci de contrôle de ses données personnelles. En utilisant toutes les dimensions d'Hofstede dans un contexte européen, nous montrons que celles-ci peuvent être réduites à trois dimensions majeures : ceci nous permet une simplification et une meilleure compréhension des phénomènes.

Notre recherche apporte donc une première contribution théorique importante dans l'identification des dimensions culturelles influençant la préoccupation pour la protection des données personnelles.

1.2. Identification d'un comportement de plainte spécifique

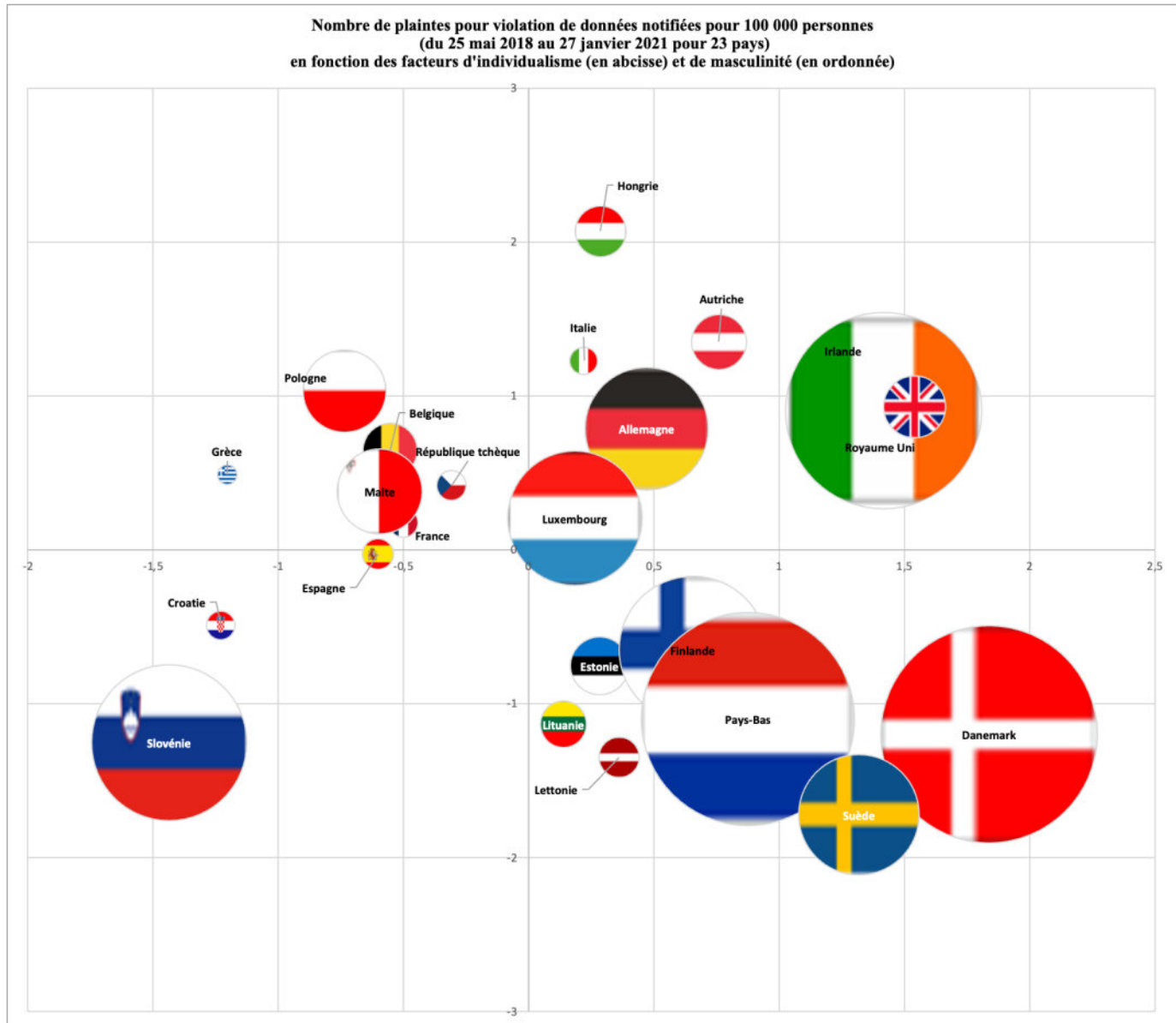
Les comportements individuels face à une violation de données personnelles ont très peu été étudiés jusqu'à maintenant (Labrecque, 2021). Cette recherche identifie la plainte pour violation de la protection des données personnelles comme un comportement spécifique dans la littérature sur les préoccupations relatives à la vie privée. Ce point est approfondi dans le chapitre 7 (pages 349-350).

2. Implications pratiques

2.1. Vers une adaptation locale des moyens d'adoption du RGPD

Notre recherche montre que les pays européens qui valorisent davantage l'individualisme (e.g., Danemark, Royaume-Uni, Suède) ont tendance à se plaindre davantage, tandis que les pays européens qui valorisent davantage la masculinité (e.g., Hongrie, Autriche, Italie) ou l'orientation à long terme (e.g., Belgique, la Lituanie, Allemagne) ont tendance à moins se plaindre pour la violation de la protection des données personnelles. En d'autres termes, des pays européens collectivistes et masculins, comme la France, enregistrent moins de plaintes pour violation de la protection des données personnelles, tandis que les pays européens individualistes et féminins, comme le Danemark ou la Suède, enregistrent plus de plaintes. Cela va dans le sens de la conclusion de Girerd-Potin et al. (2018) selon laquelle les intérêts des parties prenantes directes non financières des entreprises (par exemple, les citoyens) sont mieux pris en compte dans les pays individualistes et féminins. Pour illustration, nous représentons graphiquement les pays dans la Figure 26 ci-dessous selon leur nombre de plaintes et leurs facteurs d'individualisme (en abscisse) et de masculinité (en ordonnée).

Figure 26 : Représentation des 23 pays européens selon leur nombre de plaintes et les facteurs d'individualisme et de masculinité



En identifiant les mécanismes culturels dans la plainte pour violation de la protection des données personnelles, cette recherche fournit des recommandations pour des politiques localisées de protection de la vie privée. La mise en œuvre des politiques publiques dans une perspective plus large que les politiques nationales, telle que la perspective européenne, doit tenir compte des différences culturelles pour être efficace (Bellman et al., 2004; Milberg et al., 2000) selon l'adage : « *Think global, act local* ». Par ailleurs, tout en insistant sur la nécessité d'harmonisation européenne de la mise en œuvre du RGPD, la Commission européenne

recommande d'adapter les moyens de déploiement à l'échelle nationale, afin de modifier le comportement et le mode de pensée de tous les acteurs, avec par exemple « la conception d'outils appropriés et de formats et d'interfaces standard »⁹³ (p.10). En d'autres termes, chaque pays avance à son rythme et en coordination avec les autres, l'objectif étant que chacun parvienne au même niveau de protection des données personnelles des citoyens et de déploiement de l'ensemble des outils prévus dans le cadre du RGPD.

À titre d'exemple, les pays collectivistes, où les personnes ont tendance à moins se plaindre, devraient renforcer les ressources financières et humaines des autorités de protection des données pour développer les activités de contrôle de la conformité au RGPD⁹⁴, et favoriser les sanctions sur la base d'actions collectives. Comme nous l'avons vu en introduction, les montants des amendes prononcées dans chaque pays sont souvent inversement proportionnels au nombre de plaintes. Ces amendes sont-elles efficaces ? Quels autres moyens pourraient être développés dans le même sens ? À l'inverse, dans les pays enregistrant le nombre de plaintes le plus élevé, ces interpellations de la part des citoyens-usagers ne sont-elles pas reconnues comme un réel mécanisme de correction des pratiques en matière de vie privée ?

2.2. Vers la construction d'une typologie de pays européens

Enfin cette typologie de pays, présentée dans le paragraphe suivant, pourrait être enrichie par l'ajout d'autres indicateurs (ceci peut être une limite de notre travail). Ces indicateurs pourraient être institutionnels (rôle de la loi ou scores de confiance institutionnelle, contrôle de la corruption), socio-économiques permettant de refléter soit une maturité digitale soit une capacité éducative à porter plainte pour ce sujet (niveau de maturité digital, taux d'équipements, part des achats sur Internet, scores PISA) ou de sensibilisation au RGPD (taux de notoriété RGPD⁹⁵). Une prise en compte d'autres critères permettra d'améliorer une vision peut-être un peu simpliste de la dichotomie individualisme – collectivisme, comme l'a suggéré Dinev et al. (2006) en complétant le cadre théorique d'Hofstede avec la théorie du capital social de

⁹³ Communication de la commission au parlement européen sur la protection des données (disponible le 29 juillet 2022 à : <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0115:FIN:EN:PDF>)

⁹⁴ On note par exemple en 2022 une augmentation du budget de la CNIL et une externalisation du traitement des plaintes (<https://www.dastra.eu/fr/article/la-cnil-va-augmenter-son-budget-en-2022-pour-repondre-au-defi-du-rgpd/47508>)

⁹⁵ Special Eurobarometer 487a. *opt. cit.*

Fukuyama (1995). En effet, les formes d'individualisme (IND) et de collectivisme peuvent être très variées et l'individualisme tel que vécu dans les pays scandinaves (IND = 71 en Suède ; IND = 69 en Norvège) ou en France (IND = 71) semble assez différent. Les résultats pourraient être regroupés par zones et par hypothèses (Europe du Nord, Europe du Sud ou pays latins, pays germaniques, Europe orientale) afin de mieux préciser leurs principales caractéristiques sociales et politiques et de discuter nos résultats en regard de ces différents contextes.

3. Limites et voies de recherches

Bien entendu, notre recherche présente des limites qui indiquent des pistes de recherche futures. Certaines limites sont reprises dans le chapitre 7.

Premièrement, s'il est essentiel de mieux comprendre la plainte pour atteinte à sa vie privée, celle-ci reste un indicateur à manier avec précaution. En effet, le nombre de plaintes, même s'il est en progression, reste faible en comparaison avec le nombre d'atteintes à la vie privée et de violations de données personnelles⁹⁶. De plus, il serait intéressant d'étudier si la culture influence la nature des plaintes au-delà de leur simple volume, ce qui nécessite de recueillir des données plus détaillées sur le sujet des plaintes⁹⁷. Enfin, les recherches futures devraient également s'étendre à d'autres formes de réactions négatives aux violations de la protection des données personnelles, telles que le bouche-à-oreille ou les confrontations en face à face, qui sont plus probables dans les sociétés collectivistes (Chapa et al., 2014), ce que nous faisons dans le chapitre suivant de notre travail doctoral.

Deuxièmement, au-delà du modèle de Hofstede qui envisage l'influence de la culture, à un niveau macro et national, des recherches supplémentaires pourraient explorer les phénomènes à un niveau plus micro et psychologique, ce que nous faisons dans les chapitres suivants de notre travail doctoral. Par la suite, d'autres perspectives supplémentaires pourraient inclure des cadres conceptuels issus de l'anthropologie (e.g., Hall, 1976), de l'histoire ou de la philosophie (e.g., d'Iribarne et al., 1998).

⁹⁶ Rapport Institut Montaigne décembre 2019 « Données Personnelles, comment gagner la bataille ? », disponible à : <https://www.institutmontaigne.org/ressources/pdfs/publications/donnees-personnelles-comment-gagner-la-bataille-etude.pdf>

⁹⁷ Nous avons à plusieurs reprises été en contact avec des représentants du cabinet DLA Piper, qui n'ont pas donné suite à nos demandes.

Troisièmement, d'autres raisons peuvent intervenir dans l'explication de la variabilité dans le nombre de plaintes pour violations de données entre pays européens, comme la proximité géographique avec les centres décisionnels ou la facilité de dépôt de plainte (cf. en Annexe 6 l'interface de dépôt de plainte à priori facile d'usage sur le site Internet de l'autorité nationale irlandaise pour la protection des données personnelles). Il pourrait être intéressant de mieux les prendre en considération.

Enfin, nous suggérons de continuer à approfondir la compréhension de la notion de confiance, déterminant essentiellement de la préoccupation pour la protection de la vie privée, dans la continuité des travaux de Dinev et al. (2006) et alors que Ting-toomey & Kurogi (1998) soutiennent l'idée que les définitions des termes « confiance » et « propension à faire confiance » diffèrent d'une nation à l'autre. La possible contradiction entre notre résultat indiquant que la masculinité amène à moins se plaindre et le fait que les plaignants recensés par la CNIL sont majoritairement des hommes est également à éclairer. Pour terminer, il serait intéressant d'explorer le lien entre comportement de plainte pour atteinte à la vie privée et comportement de dénonciation entre voisins (assez habituel au Royaume-Uni ou dans les pays du nord de l'Europe ; beaucoup débattus dans le cadre de la gestion de la crise sanitaire du Covid-19), qui par extension a donné lieu au développement de la *cancel culture* (e.g., pratique visant à dénoncer publiquement certains comportements inadmissibles, comme le mouvement #metoo).

Synthèse de l'essai 1

Dans ce premier essai portant sur l'influence de la culture nationale sur le comportement de plainte pour violation de données personnelles, nous montrons que les individus issus de pays européens valorisant davantage la féminité (i.e., l'égalité des sexes et les soins communautaires) ont tendance à se plaindre davantage que ceux issus de pays européens valorisant davantage l'individualisme (i.e., une préférence pour l'autonomie, l'indépendance et la liberté individuelle, privilégiées au collectivisme et à la défense du groupe social) ou la tradition.

Cependant, il nous est nécessaire de continuer l'observation des effets culturels à d'autres niveaux d'observation (mésos dans le chapitre 5 et micro dans le chapitre 6), d'identifier les autres possibilités de réponse face à une violation de données personnelles et d'explorer les mécanismes sociologiques et psychologiques reliant culture et réponse.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

Protection
des données
personnelles

Réponses des
consommateurs
insatisfaits

Culture
et valeurs



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :
Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :
Influence
des normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :
Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 5. Essai 2 - Influence des normes socio-culturelles

sur les réponses à une violation de données personnelles



Résumé

Plusieurs actions collectives pour le respect du Règlement Général sur la Protection des Données personnelles (RGPD) sont menées depuis son entrée en vigueur. Alors que la protection de la vie privée est un droit individuel, nous nous interrogeons sur les motivations des personnes engagées collectivement pour le respect de ce droit. Cet essai vise à comprendre quelles valeurs sont partagées collectivement par ces personnes. Mobilisant des entretiens approfondis (N=15), et à la lumière de la théorie de la pratique (Bourdieu, 1972; Giddens, 1984), nous mettons en lumière, d'une part, que la défense d'une équité sociale est une motivation essentielle à un engagement pour le respect de la vie privée, et, d'autre part, que la protection de la vie privée est une pratique sociale. Cette dernière se développe autour de structures mobilisant des valeurs (idéaux), des moyens (matériaux), et des formes de compétences (e.g., sentiment d'efficacité). Un développement équilibré entre idéaux, moyens et formes de compétences permet l'adoption d'une réponse active face à une violation de données personnelles. Enfin, les défenses de sa liberté ou de sa sécurité individuelle sont deux motivations supplémentaires à ces réponses. Cette recherche offre un éclairage théorique novateur à la question de la protection de la vie privée : premièrement, elle l'envisage comme une pratique sociale, et non comme une pratique individuelle, éliminant l'idée que les individus sont les seuls responsables. Deuxièmement, elle remet en question la primauté de l'individualisme comme valeur fondatrice de la protection des données personnelles.

Biographie de l'essai : Une communication extraite de ce chapitre sera présentée au Congrès de l'afm 2023 (Vannes, France, du 10 au 12 mai 2023).

Section 1. Introduction

En mai 2018, 12.000 personnes signent une pétition à l'initiative de la Quadrature du Net (association de défense des droits et libertés sur Internet) contre les géants du numérique (e.g., Facebook, Amazon) pour non-respect du RGPD, rassemblant en six semaines plus de plaintes que la CNIL sur l'année écoulée⁹⁸. En juillet 2020, l'accord de transfert de données personnelles européennes vers les États-Unis, le *Privacy Shield*, est invalidé sur l'initiative de l'association *None of Your Business* portée par Marx Shrems⁹⁹ (association qui a aussi permis de rendre illégale début 2022 en Europe l'utilisation de Google Analytics). En septembre 2021, l'association de défense des consommateurs UFC-Que choisir envisage de lancer des actions collectives en justice contre les violations de données personnelles¹⁰⁰. En août 2022, une action collective (*class action*) est portée contre Oracle par le régulateur irlandais, plusieurs avocats et spécialistes de la protection de la vie privée « au nom des internautes du monde entier qui ont été victimes des violations de la vie privée commises par Oracle »¹⁰¹.

Plusieurs actions collectives sont menées pour le respect du RGPD, depuis son entrée en vigueur en Europe en mai 2018. Ceci nous interroge sur les motivations des personnes engagées collectivement pour le respect de la vie privée, alors que la protection de la vie privée est un droit individuel. Protéger ses données personnelles relève de l'action individuelle que ce soit techniquement (e.g., bloquer des marqueurs de traçage en ligne) ou légalement (les moyens de recours au droit comme le retrait de ses données ou la plainte auprès des régulateurs étant individuels). En particulier, nous questionnons le rôle des valeurs motivationnelles (culturelles et éthiques) dans les actions de protection de la vie privée en ligne (Son & Kim, 2008). Jusqu'à présent, la littérature se concentre principalement sur l'influence de l'individualisme (i.e., une préférence pour la défense de ses propres intérêts ; Miltgen & Peyrat-Guillard, 2014) dans la préoccupation pour le respect de la vie privée, mais révèle des contradictions dans les effets des dimensions (Hofstede, 2001; Rokeach, 1973), pouvant s'expliquer par des phénomènes

⁹⁸ https://www.laquadrature.net/2018/05/28/depot_plainte_gafam/

⁹⁹ <https://www.lesechos.fr/tech-medias/hightech/accord-surprise-sur-le-transfert-des-donnees-personnelles-entre-leurope-et-les-etats-unis-1396225>

¹⁰⁰ <https://www.rtl.fr/actu/sciences-tech/vol-de-donnees-a-l-aphp-plainte-action-collective-quels-recours-pour-les-victimes-7900074390>

¹⁰¹ <https://www.lemondeinformatique.fr/actualites/lire-une-class-action-vise-oracle-pour-collecte-massive-des-donnees-personnelles-87759.html>

insuffisamment observés à différents niveaux, et appelant de fait à davantage de recherches (Martin et al., 2020).

Dans ce contexte, notre recherche propose d'explorer les valeurs motivationnelles au niveau des groupes et des collectifs engagés pour la protection de la vie privée, i.e., à un niveau méso. Plus précisément, le niveau méso est le niveau d'observation des organisations ou associations (méso-social) et des sphères privées (micro-social) (Desjeux, 2006). Le niveau méso est un niveau intermédiaire entre des niveaux macro (nationaux et institutionnels) ou micro (psychologique et individuel). Le niveau méso n'a, à notre connaissance, jamais été questionné concernant la protection de la vie privée informationnelle (i.e., vie privée concernant les informations partagées comme les communications et données personnelles ; Clarke, 1999). Or le lien entre les actions conduites à des niveaux macro et micro réside dans les interdépendances entre les acteurs (Liljenstrom & Svedin, 2005) et provient des unités sociales méso (Dopfer et al., 2004). Ceci semble d'autant plus vrai pour les actions de protection de la vie privée qui résultent d'une tension entre macro-pouvoirs des institutions (contrôle des réglementations de la protection des données et de l'économie numérique) et micro-pouvoirs individuels (gestion des données personnelles) (Chaudhury & Albinsson, 2015). Explorer le niveau méso concernant les actions pour le respect de la vie privée pourrait permettre ainsi d'apporter un nouvel angle de vision.

Interroger l'influence des normes culturelles à un niveau méso (niveau de construction des dynamiques sociales) revient à identifier les principales valeurs partagées au sein de ces groupes sociaux et à éclairer le rôle des valeurs dans la construction de pratiques sociales, i.e., des façons d'agir et de se conduire, partagées et reconnues par le groupe (Bourdieu, 1972; Giddens, 1984; Turner, 1994). Dans le cas présent, la pratique sociale considérée renvoie aux actions face à des violations de données personnelles. Ceci nous amène à interroger la manière par laquelle le droit privé et individuel de la protection de la vie privée et des données personnelles est construit et développé de façon collective, à travers la mise en place de pratiques sociales de protection de la vie privée.

Par voie de conséquence, cet essai pose la question suivante : **Comment des valeurs, structurant des pratiques sociales collectivement partagées, peuvent-elles influencer les réponses à la violation d'un droit individuel, i.e., la protection de ses données personnelles ?** Pour répondre à cette question, notre recherche cherche à identifier d'une part les principales valeurs en jeu, et d'autre part le rôle de ces valeurs au sein de pratiques sociales.

Cette recherche ayant une visée exploratoire, nous adoptons une approche qualitative. Pour cela, nous avons conduit plusieurs entretiens approfondis (N=15) avec des personnes engagées pour la protection des données personnelles (à titre individuel ou au sein de collectifs). Ces personnes ont été interrogées sur leurs pratiques, leurs motivations et les réponses apportées face à une violation de leurs données personnelles, au cours d'entretiens semi-directifs permettant la construction de chaînages cognitifs. Le corpus obtenu a été analysé à l'aide d'une analyse thématique classique (Allard-Poesi, 2003; Dumez, 2021) et de chaînage cognitif (Reynolds & Gutman, 1988; Valette-Florence et al., 2003). Les résultats sont présentés selon la structure de Giddens (1984), nous indiquant que les pratiques sociales se trouvent à l'intersection de matériaux (e.g., technologies, moyens techniques), de compétences (e.g., savoir-faire, croyances), et de valeurs (e.g., symboles, aspirations).

Nous montrons que la défense d'une équité sociale est une motivation essentielle pour s'engager en faveur de la protection de données personnelles. Plus précisément, trois motivations culturelles dominantes sont identifiées : (i) l'équité sociale (i.e., défendre une diversité et une égalité sociale, permettre, à l'aide de moyens techniques aux plus vulnérables de garder des informations confidentielles et de moyens institutionnels, de faire vivre et d'appliquer le droit, et, à l'aide d'actions sociales, de protéger un bien commun) ; (ii) la liberté (de choix, en permettant à chacun par des voies techniques ou réglementaires de garder son jardin secret) ; (iii) la sécurité personnelle (à travers la protection de son autonomie et de son intimité).

De plus, les actions de protection des données personnelles reposent sur des dynamiques collectives et la protection de la vie privée est envisagée comme une pratique sociale, mobilisant des moyens techniques, des formes de compétences et croyances individuelles (e.g., sentiment d'efficacité) ou collectives (qui apportent connaissance et support) et des valeurs. Si les valeurs culturelles sont un moteur motivationnel puissant pour être engagé pour la protection de ses données personnelles, elles se heurtent souvent à un manque de moyens techniques (i.e., outils ergonomiques et accessibles protecteurs de la vie privée), à des compétences limitées (i.e., *privacy literacy* ; Bartsch & Dienlin, 2016), à un sentiment d'inefficacité, voire une certaine résignation et fatigue (i.e., *privacy fatigue* ; Choi et al., 2018). Ce déséquilibre entre valeurs motivationnelles, matériaux disponibles et compétences freine le développement de pratiques sociales de protection de la vie privée. En revanche, le développement d'un savoir (articulé autour d'une alphabétisation numérique et d'une réduction de la distance psychologique avec les risques liés à la violation des données personnelles ; Trope & Liberman,

2010), et d'un pouvoir (grâce aux développements d'outils techniques accessibles et de collectifs permettant la formation, l'entraide et le soutien) minimise l'importance des idéaux et des valeurs culturelles. **En somme, les individus agissent par des moyens collectifs, et souvent pour des raisons collectives dans un souhait d'équité sociale.** Si la protection des données personnelles est bien un droit individuel, celui-ci ne peut pas s'exercer individuellement, mais collectivement. Ce constat est d'autant plus vrai dans le cas d'une violation grave de données personnelles : « tous pour un, un pour tous », un individu seul est démuni face à une violation majeure de ses données.

C'est pourquoi cette recherche interroge sur l'importance d'une préférence culturelle pour l'individualisme (i.e., la défense de ses propres buts et intérêts ; Hofstede, 2001), souvent mobilisée pour expliquer les variations culturelles dans la préoccupation pour la protection de la vie privée (e.g., Miltgen & Peyrat-Guillard, 2014). Nous remettons ainsi en question le rôle de l'individualisme comme valeur fondatrice du droit à la vie privée, et nous distinguons l'individualisme de l'individualité (terme choisi pour recouvrir les notions d'autonomie et d'intimité). La protection de son individualité, de son intimité et de son autonomie, apporte une sécurité personnelle, réelle ou perçue (constitutive d'un imaginaire de sécurité). En pratique, les pouvoirs publics ou les entreprises pourraient davantage mobiliser les schémas motivationnels identifiés, et communiquer sur les notions d'équité, de liberté et de sécurité personnelle afin de mobiliser une conscience collective. Le développement de plaintes collectives dans le cas de violations de données personnelles pourrait également être facilité.

De plus, cette recherche apporte un éclairage théorique totalement novateur grâce à l'approche méso adoptée. En effet, à notre connaissance, la protection des données personnelles n'a jamais été envisagée comme une pratique sociale (contrairement à la vie privée « physique » qui est une construction sociale et collective ; Altman, 1977; Ariès & Duby, 1985). Cette recherche initie des possibilités de développements théoriques aux impacts sociétaux forts, à l'instar des recherches en sociologie de la santé : celles-ci mobilisent la théorie de la pratique afin de comprendre les leviers permettant par exemple de favoriser les pratiques sportives, considérant celles-ci comme des pratiques sociales dépendantes de l'environnement d'habitation, et non comme des pratiques individuelles, éliminant ainsi l'idée que les individus sont les seuls responsables de leur propre état de santé (Maller, 2012). Cette approche permet aussi d'inscrire la protection des données personnelles dans une dynamique de consommation éthique et responsable (Parguel et al., 2018) car la théorie de la pratique cherche à expliquer comment les

êtres sociaux construisent et transforment le monde dans lequel ils vivent, et comment des relations se mettent en place entre l'action humaine individuelle et une entité globale systémique ou institutionnelle (Ortner, 2006).

Section 2. Fondements théoriques de la recherche

Cet essai vise à identifier tant les principales valeurs motivationnelles en jeu pour les personnes engagées dans le respect du droit à la vie privée que le rôle de ces valeurs au sein de pratiques sociales. C'est pourquoi dans cette partie, nous éclaircissons les fondements conceptuels de notre recherche, en commençant par les valeurs motivationnelles (1). Nous précisons ensuite les réponses engagées pour le respect du droit à la vie privée, notamment face à des violations de données personnelles (2). Puis, nous exposons les grands principes de la théorie de la pratique (3) et en particulier le rôle des croyances, consciences et facteurs influençant les actions et les pratiques (4).

1. Valeurs et motivations socio-culturelles

Comme précisé précédemment dans le manuscrit (cf. chapitre 2 section 3 – pages 126 à 154), un système de valeurs est un ensemble de règles apprises permettant à une personne de choisir entre des alternatives, à résoudre des conflits et à prendre des décisions (Rokeach, 1973), basé sur le principe qu'un mode de conduite ou un état final d'existence est préférable à un autre. Les valeurs apportent un cadre normatif, éthique, voire politique ou religieux, à l'action. Les valeurs permettent de classer les actions selon des idéaux (e.g., de générosité, de sécurité).

De plus, comme indiqué page 137, les valeurs résultent de processus de socialisation ou apprentissage social (Bandura, 1977; Bourdieu, 1979) qui consistent à apprendre en observant des modèles, imiter et reproduire efficacement certains comportements sociaux, ou encore des interactions individuelles (Sapir, 1921). Tout l'intérêt de cet essai est donc d'identifier les valeurs partagées par des personnes toutes engagées pour la protection de la vie privée, sous différentes formes.

Ainsi, les valeurs peuvent agir et être différentes entre les différents niveaux (macro, méso, micro). Pour exemple, Chandrasekharan et al. (2018) étudient l'effet de normes culturelles dans les modérations de discussions des communautés « subreddits » (i.e., des communautés de discussions en ligne *ex nihilo*, modérées par ses membres et rassemblées dans Reddit¹⁰²).

¹⁰² www.reddit.com

Sur la base de 2,8 millions de commentaires supprimés par les modérateurs, cette recherche distingue :

- les normes macro-universelles (e.g., misogynie, racisme, homophobie),
- les normes méso (appliquées par chaque sous-groupe de « subreddits » ; e.g., ne pas partager d'anecdotes personnelles),
- et des normes micro individuelles (régulant les comportements de chacun).

L'objectif de notre recherche est d'étudier l'influence de ces valeurs sur les comportements de réponses des personnes engagées, ce que nous précisons à présent.

2. Réponses engagées pour la protection des données personnelles

2.1. Engagement face à une violation de données personnelles

L'engagement est défini comme l'« acte par lequel on s'engage à accomplir quelque chose » ou le « fait de prendre parti sur les problèmes politiques ou sociaux par son action et ses discours »¹⁰³. En sciences de gestion ou en marketing, la notion d'engagement intègre des dimensions de satisfaction, d'implication et de motivation (Schaufeli, 2013), précisant que l'engagement peut être psychologique ou comportemental (Harmeling et al., 2017).

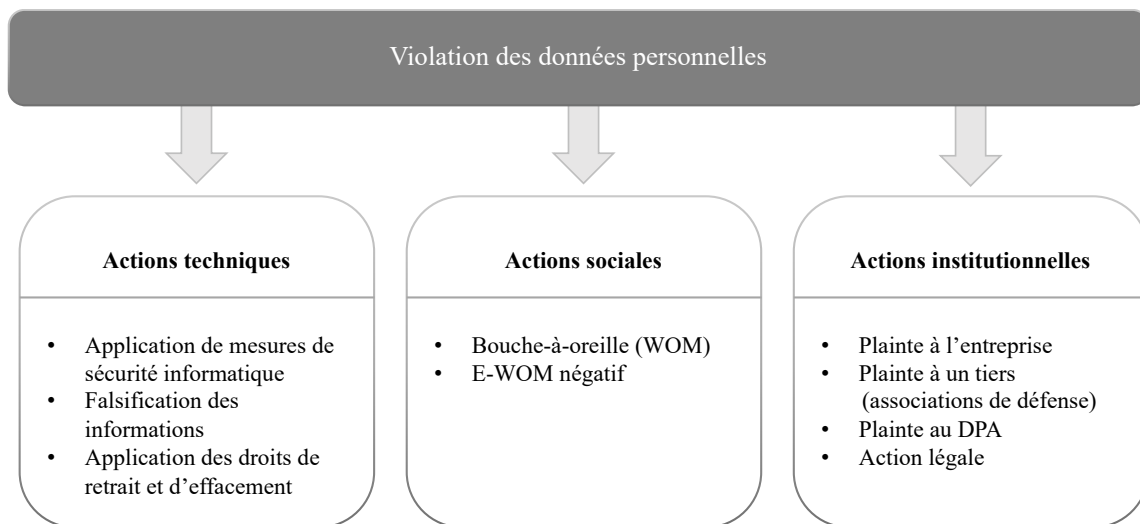
De ce fait, dans le cadre de notre recherche, nous cherchons à interroger des personnes engagées pour la protection de la vie privée, i.e., manifestant leur intérêt pour la protection de la vie privée à travers un « passage à l'acte ». Ce « passage à l'acte » regroupe tout type d'actions, depuis une vigilance simple dans la gestion de ses interactions digitales jusqu'à une action fortement militante avec la conduite de poursuites judiciaires. Nous classifions ces actions en trois catégories : sociales, techniques ou institutionnelles, que nous précisons dans le paragraphe suivant.

¹⁰³ <https://www.larousse.fr/dictionnaires/francais/engagement/29510>

2.2. Réponses face à une violation de données personnelles

Nous avons dans le cadre de notre thèse de doctorat (chapitre 2, section 2, paragraphe 2.2.1) proposé une première actualisation des différentes modalités de réponses, en incluant différentes modalités supplémentaires : (i) l'application de mesures de sécurité, telles que l'authentification et le contrôle d'accès (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018), (ii) le recours aux dispositions offertes par le RGPD, comme les droits d'effacement ou de restitution, (iii) les différents recours légaux (Mamonov & Benbunan-Fich, 2018; Romanosky et al., 2013). Nous avons donc proposé le modèle ci-après (cf. Figure 27) organisé autour de trois sections : actions techniques, actions sociales et actions institutionnelles. Notre recherche vérifie et actualise cette typologie.

Figure 27 : Réponses face à une violation de données personnelles



3. Théorie de la pratique

Dans ce paragraphe, nous précisons les principes généraux de la théorie de la pratique (3.1.), l'approche de la théorie de la pratique vue par Bourdieu (3.2.), ainsi que l'approche plus structurelle de la pratique de Giddens (3.3.) et nous illustrerons l'utilisation de la théorie de la pratique dans plusieurs mises en application (3.4.).

3.1. Principes généraux de la théorie de la pratique

Une pratique sociale est « comprise au sens large comme une compréhension tacite partagée par un groupe » (Turner, 1994, p.1), une façon de faire, une manière particulière d'agir, une conduite humaine ordinaire qui a été intégrée dans le temps à travers des interactions avec des personnes et des choses et au fur et à mesure de l'expérience au monde, une action (individuelle ou collective) socialement transmise ou envisagée dans un contexte social. Notre recherche envisage la protection des données personnelles comme une pratique sociale.

De plus, la pratique est inscrite dans le concret, dans le monde de l'action (*praxis*) par opposition au monde abstrait des idées (*theoria*). Mais, la pratique se différencie de l'action. Elle regroupe des « habitudes, des actions régulières, des dispositions (compétences ou croyances) à agir, des activités, des manières de faire » (Catinaud, 2015, p.28) et se distingue de l'action par sa répétition et sa significativité (i.e., permettant de donner du sens à l'action).

Par ailleurs, le temps est un élément essentiel de la pratique car non seulement elle se construit et se développe dans le temps (notion de structure temporelle de l'expérience) mais elle fait et construit aussi le temps (Bourdieu, 2016).

Tableau 35 : La théorie de la pratique

Définition de la théorie de la pratique	- Un ensemble d’actions et de manières de faire, et partagées et comprises tacitement au sein d’un groupe social
Principaux concepts théoriques	- Habitus : une « structure structurante, qui organise les pratiques et la perception des pratiques » (Bourdieu, 1979, p.191) - Structure : le résultat d’un processus de construction actif qui est accompli et composé par les actions des agents (Giddens, 1976)
Composants de la structure	- Matériaux : des entités physiques tangibles - Compétences : formes de compréhension, de connaissance ou de croyance - Valeurs : significations symboliques
Exemples d’application	- Pratiques sportives (sociologie de la santé) - Pratiques environnementales - Pratiques de déplacement intra-urbain
Place des valeurs dans les pratiques	- Les valeurs occupent une place mineure dans la théorie de la pratique qui privilégie l’action formelle (descriptive) à l’action normative (i.e., guidée et normée par des valeurs), qui remet en question une totale rationalité de l’action, voire qui refuse une posture tournée vers un idéalisme.

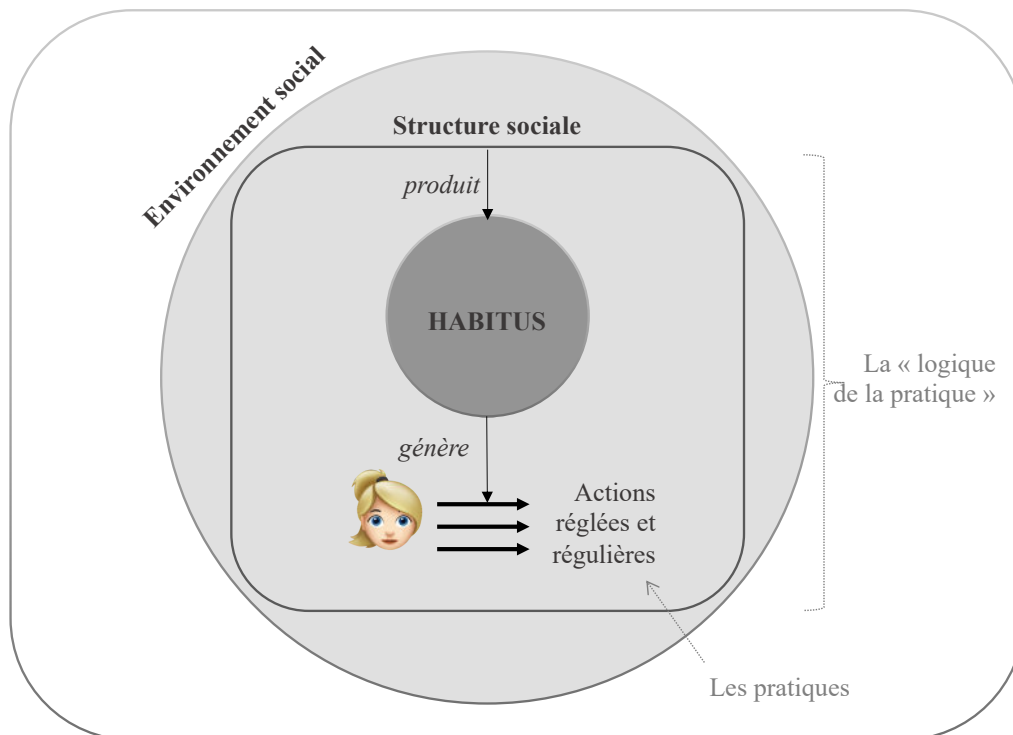
Nous affinerons, par la suite, les fondements conceptuels de la théorie de la pratique, ses composants dont la place des valeurs, comme précisé dans le Tableau 35 ci-dessus.

La pratique a été appréhendée en philosophie (Heidegger, 1927; Wittgenstein, 1958), en épistémologie (Kuhn, 1962; Latour & Woolgar, 1979), et en sociologie (Bourdieu, 1972; Giddens, 1984; Schatzki, 1996; Turner, 1994), champ dans lequel notre recherche s’inscrit. Les différents courants de pensée sociologiques reposent sur deux principales idées. D’une part, l’action humaine est appréhendée par opposition à une vision individualiste (i.e., les phénomènes sociaux sont la somme d’actions individuelles et rationnelles ; Boudon, 1984) et à une vision holistique (i.e., les actions individuelles sont prédéterminées par des structures sociales macro, les agents sociaux n’étant pas alors en capacité de modifier les structures par leurs actions quotidiennes ; Durkheim, 1894). D’autre part, il n’est pas possible d’appréhender le réel (l’action et la pratique) par la théorie (l’abstraction et la contemplation) et tout observateur qui voudrait analyser l’action de l’extérieur (de façon stable et délimitée) dénaturerait le processus de pratique dynamique et ouvert.

3.2. Théorie de la pratique selon Bourdieu

À travers son ouvrage « Esquisse d’une théorie de la pratique », Bourdieu (1972) a marqué le courant de la théorie de la pratique en sociologie. Chez Bourdieu, la théorie de la pratique sert à étudier les comportements des agents sociaux en situation, la relation liant ces comportements avec les traditions et les positions sociales et culturelles des individus, et la façon dont les structures sociales sont produites et reproduites à travers leurs actions. Bourdieu définit le concept d’*habitus*, i.e., « une structure structurante, qui organise les pratiques et la perception des pratiques » (Bourdieu, 1979, p.191), compris comme des capacités à engendrer des habitudes sociales, des dispositions intériorisées et des apprentissages (au sein d’institutions). Les *habitus* sont composés de conventions sociales, de normes et de valeurs qui guident nos actions quotidiennes. En d’autres termes, la pratique est un cadre général composé de structures extérieures (environnement social) et de structures intérieures (sens donné) qui va générer des pratiques (cf. Figure 28) : ainsi la théorie de la pratique est un mode de génération des pratiques. Enfin, trois notions clés composent la génération des pratiques : le temps et les rythmes sociaux, la routine et les infrastructures matérielles (Dubuisson-Quellier & Plessz, 2013).

Figure 28 : Structure sociale et *habitus* de Bourdieu (Catinaud, 2015)

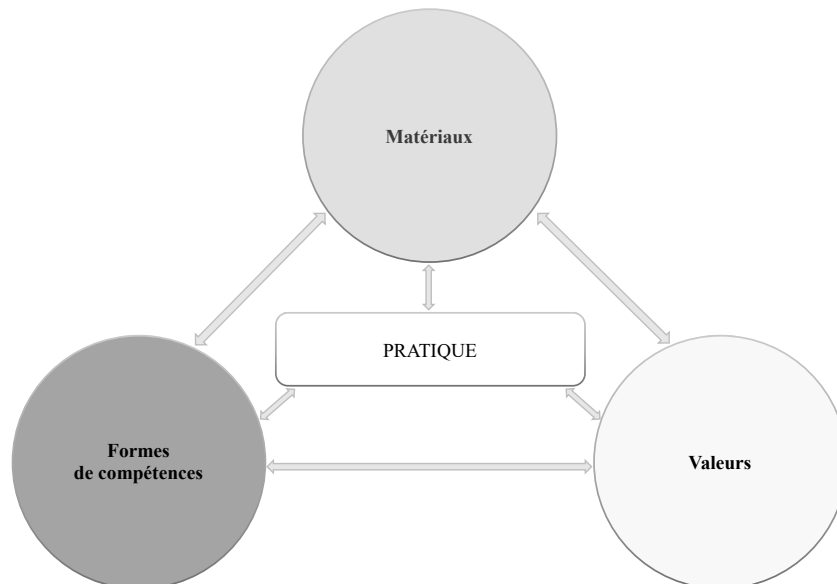


3.3. Théorie de la pratique et la notion de structure de Giddens

Giddens se distingue de Bourdieu par une approche plus théorique que pratique. La notion de structure est également présente chez Giddens : une structure est le résultat d'un « processus de construction actif qui est accompli et composé par les actions des sujets actifs » (Catinaud, 2015, p.62), i.e., un mécanisme de structuration opérant par l'exercice d'une pratique. Une structure est un ensemble de règles et de ressources (e.g., disposition, compétence, savoir-faire, habitude, motivation, norme sociale ou culturelle) encadrant les pratiques des individus, ces règles et ressources étant elles-mêmes redéfinies de façon dynamique et récursive par l'exercice des pratiques. Chez Giddens, la pratique se trouve à l'intersection entre (cf. Figure 29) :

- des matériaux (e.g., des technologies, des entités physiques tangibles, des infrastructures, des supermarchés, des réseaux sociaux, des applications mobiles),
- des compétences (i.e., différentes formes de compréhension, de connaissance, de croyances, de facteurs qui influencent les actions et les pratiques), que nous nommons par la suite « formes de compétences » pour reprendre l'expression d'Elizabeth Shove (Shove et al., 2012),
- et des valeurs (e.g., significations symboliques, idées et aspirations).

Figure 29 : Structure de la théorie de la pratique de Giddens



Les dimensions sociales de la pratique sont (i) associées à des structures matérielles et techniques, à travers les matériaux, (ii) font l'objet de prescriptions ou exigences sur la manière de faire à travers les compétences ou croyances, (iii) et sont dotées d'un sens à travers les valeurs. Nous préciserons par la suite comment les concepts de matériaux, compétences et valeurs se traduisent et s'appliquent dans le cas des réponses face aux violations de données personnelles.

Chez Giddens, la pratique est récursive. Ce mécanisme de structuration récursif compose la « dualité du structurel ». Cette dualité est d'une part passive (cachée) : elle est inscrite dans la mémoire des individus, qui la mobilisent pour l'accomplissement de pratiques. Elle est d'autre part active (visible) : elle se manifeste à travers les actions concrètes des individus.

La théorie de la pratique a été mobilisée dans différents contextes, que nous illustrons dans le paragraphe suivant.

3.4. Mise en application de la théorie de la pratique

La conceptualisation de pratiques sociales permet de comprendre les dynamismes dans le cas de certains phénomènes sociétaux (e.g., santé publique, sécurité routière, violations de données sensibles). Pour exemple, la théorie de la pratique a été mobilisée en sociologie de la santé pour comprendre les leviers permettant de favoriser les pratiques sportives, considérant les pratiques sportives comme des pratiques sociales et des caractéristiques clés d'environnements (quartiers d'habitation), et non comme des pratiques individuelles, éliminant ainsi l'idée que les individus sont les seuls responsables (et peuvent donc être blâmés) de leur propre état de santé (Maller, 2012). La théorie de la pratique a également été utilisée dans le contexte des pratiques environnementales et durables (Shove, 2011; Shove et al., 2012). Enfin de façon générale, la théorie de la pratique est un éclairage théorique relativement bien adapté aux pratiques de consommation, qui permet de saisir les conditions de changement dans les pratiques et ainsi « nourrir une réflexion importante de l'action publique qui vise à encadrer des pratiques, qu'il s'agisse de pratiques en matière de santé, d'alimentation, de conduite automobile ou face à l'addiction, en dépassant les approches fondées sur l'incitation individuelle » (Dubuisson-Quellier & Plessz, 2013, p.1).

Dans cet essai, nous appliquons la théorie de la pratique au cas des violations de données personnelles. Nous rapprochons les réponses à ces violations au concept de « matériaux » mobilisé par Giddens, et les facteurs influençant ces réponses au concept de « compétences », que nous précisons dans le paragraphe suivant.

4. Facteurs influençant les réponses pour la protection de la vie privée

Pour Giddens, une compétence est une forme de compréhension, de connaissance, de croyances, c'est-à-dire un ensemble de facteurs qui influencent les actions et les pratiques, et que nous précisons dans cette partie. Comme nous l'avons indiqué page 224, nous choisissons de les nommer « formes de compétences » pour reprendre l'expression d'Elizabeth Shove (Shove et al., 2012). Ces formes de compétences sont similaires aux différents antécédents que nous avons pu identifier dans la revue de littérature (e.g., antécédents aux actions de protection de la vie privée, antécédents aux comportements de plainte) à la différence que les formes de compétence sont liées et non hiérarchisées aux valeurs et aux matériaux : ce ne sont pas les formes de compétences (« antécédents ») qui influencent les valeurs ou les matériaux mais les trois éléments évoluent en s'influencent mutuellement.

En dehors de cela, nous nous référons aux antécédents identifiés dans la revue de la littérature pour identifier les formes de compétences. Nous faisons alors état des recherches ayant identifié les facteurs influençant les réponses de protection de la vie privée, à travers trois paragraphes : les antécédents aux réponses de protection de la vie privée identifiés par Son & Kim (2008) (4.1.), les effets psychologiques des violations de données personnelles (4.2.) et les autres antécédents à ce jour insuffisamment explorés (4.3.).

4.1. Antécédents aux réponses de protection de la vie privée

Son & Kim (2008) identifient trois antécédents aux réponses pour la protection des données personnelles. Premièrement, **la préoccupation pour la protection de données personnelles** (*information privacy concern* ; Smith et al., 2011; Westin, 1967), i.e., la possibilité pour un individu de contrôler l'utilisation potentielle par des tiers de ses données personnelles (Belanger

et al., 2002; Westin, 1967). Plusieurs proxys permettent de mesurer le degré de préoccupation pour la protection de données personnelles, reprenant les dimensions de (i) collecte, utilisation secondaire non autorisée, accès inapproprié et erreurs (Smith et al., 1996), (ii) collecte, contrôle et sensibilisation (Malhotra et al., 2004), ou (iii) utilisation de mes données à des fins de ciblage commercial et reconstitution de profils individuels (Miltgen et al., 2016). En somme, deux dimensions phares caractérisent la préoccupation pour la protection de données personnelles : le contrôle (perçu de l'usage de ses données) et la transparence (des entreprises dans la collecte ou l'usage des données).

Deuxièmement, la **justice perçue**, considérant la justice comme centrale dans tout échange social. La théorie de la justice (Rawls, 1971) différencie les justices perçue (i.e., le degré de justice perçu par un utilisateur dans sa relation avec un fournisseur), distributive (i.e., le degré perçu de bonne répartition des bénéfices et avantages entre l'utilisateur et le fournisseur), procédurale (i.e., le degré de clarté, transparence et bon respect des procédures de contrôle de ses données personnelles) et interactionnelle (i.e., le degré d'honnêteté et de confiance perçus dans le traitement de ses données personnelles). Dans le contexte de la protection des données personnelles, le contrôle et la transparence (caractérisant l'*information privacy concern*) font référence à la justice procédurale alors que la collecte ou l'usage des données font référence à la justice distributive (Eggers et al., 2022). Cela se traduit dans nos législations par les obligations de demande de consentement de l'utilisateur (justice procédurale), et par les droits de retrait et d'effacement (justice distributive).

Troisièmement, les **bénéfices sociétaux de la plainte**, i.e., le degré selon lequel un utilisateur perçoit que sa plainte pour protection de sa vie privée en ligne pourrait bénéficier à d'autres utilisateurs en leur évitant d'être victime de la même manière (faisant référence aux théories des lanceurs d'alerte – *whistleblowing* – indiquant que les dénonciations faites par des employés concernant de mauvaises pratiques managériales proviennent essentiellement d'une volonté de protéger d'autres salariés des mêmes mauvaises pratiques ; Dozier & Miceli, 1985). Son & Kim (2008) identifient les bénéfices sociétaux comme étant un facteur influençant uniquement le comportement de plainte.

4.2. Effets psychologiques des violations de données personnelles

Par ailleurs, plusieurs recherches portant spécifiquement sur les violations de données personnelles identifient d'autres antécédents et effets psychologiques :

- Le **sentiment de rupture de contrat social**, i.e., le sentiment d'une rupture contractuelle avec une entreprise responsable de sécuriser les données collectées (Labrecque, 2021), évaluées selon des critères de propriété, de degré d'intimité ou de valeur des données (Krafft et al., 2021) ;
- La **perte de confiance** (Bansal & Zahedi, 2015) provoquée par la violation de données (pouvant varier selon le degré de préoccupation pour la protection de ses données personnelles ; Bansal et al., 2015).
- Le **stress** et les émotions négatives causées par la violation de données (Labrecque, 2021) ;
- La **vulnérabilité ressentie**, due à la compréhension que les dispositions des entreprises en matière de transparence et de contrôle ne sont pas garanties (Martin, 2018).

4.3. Voies de recherche

D'autres facteurs restent à explorer (Li, 2012). En particulier, l'**auto-efficacité** (*self-efficacy*) fait référence à la croyance d'un individu en sa capacité à exécuter les comportements nécessaires à la réalisation de performances spécifiques (Bandura, 1977). La *self-efficacy* a été adaptée à la *privacy*, avec le concept de *privacy self-efficacy*, i.e., l'évaluation que chacun fait de sa capacité à protéger sa vie privée en ligne (Mamonov & Benbunan-Fich, 2018). L'auto-efficacité est une dimension souvent mentionnée théoriquement comme jouant un rôle dans les réactions face à des menaces sur les données personnelles (Adhikari & Panda, 2018). Quelle que soit la technologie concernée, l'auto-efficacité renforce les comportements de protection (Baker-Eveleth et al., 2021) à travers un mécanisme d'évaluation – *coping* - de la menace potentielle sur les données personnelles Cloarec (2022). Enfin, selon Bandara et al. (2021), les personnes autonomes et compétentes en matière de vie privée (*empowered*) ne sont pas influencées dans leurs intentions comportementales par la distance psychologique avec la préoccupation pour la protection de la vie privée.

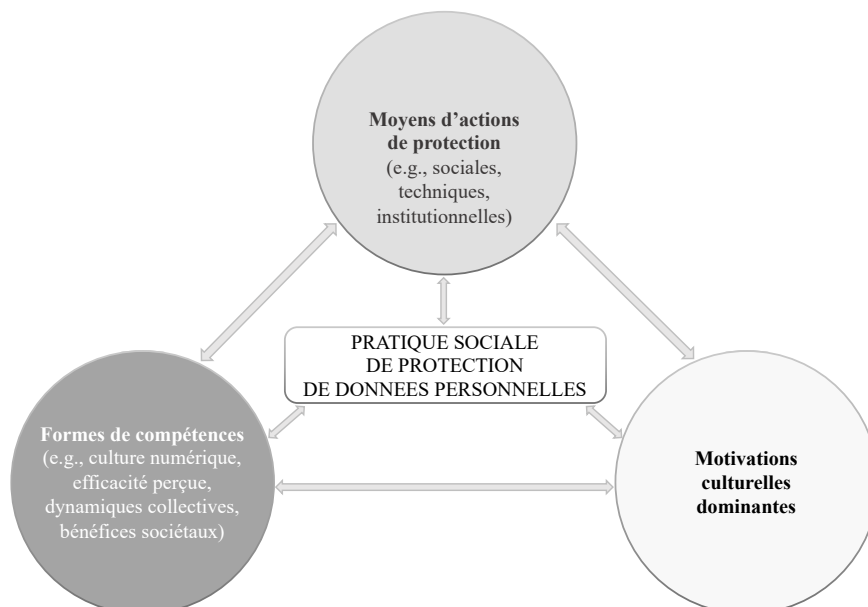
Ceci nous amène à considérer également le concept de **distance psychologique** (Trope & Liberman, 2010), i.e., la distance franchit mentalement pour se représenter un objet ou un fait. Il a été en effet montré que la préoccupation pour la protection de la vie privée était un concept de « haut niveau » (Hallam & Zanella, 2017), distant and abstrait (Bandara et al, 2018) ; et Bandara et al. (2021) montrent que la distance psychologique affaiblit la relation entre préoccupations en matière de vie privée et comportement défensif.

Pour conclure, si notre recherche permet probablement d'identifier d'autres antécédents, elle a aussi pour objectif de comprendre l'influence des valeurs culturelles sur le comportement de protection face à des violations de données personnelles. Nous précisons donc dans le paragraphe suivant les valeurs culturelles.

*

Dans cet essai, nous explorons l'influence des valeurs sur les actions de protection de la vie privée à un niveau méso. Premièrement, cette recherche vise à identifier les principales valeurs (i.e., croyances qui donnent un sens à l'action ; Rokeach, 1973) partagées par ceux qui protègent activement leur vie privée, soit par des moyens techniques (e.g., des messages cryptés), soit par des actions sociales (e.g., la sensibilisation des proches), soit par des actions institutionnelles (e.g., une plainte auprès de l'autorité de protection des données) (Son & Kim, 2008). Deuxièmement, et en s'appuyant sur la théorie de la pratique (Bourdieu, 1972; Giddens, 1984), cette recherche vise à mettre en lumière le rôle des valeurs dans la construction des pratiques sociales, i.e., des manières d'agir et de se comporter qui sont partagées et reconnues socialement par le groupe. En particulier, les pratiques sociales se situent à l'intersection de valeurs (e.g., symboles), de matériaux (e.g., technologies, moyens techniques) et de compétences (e.g., savoir-faire, croyances) (Giddens, 1984) : cf. Figure 30.

Figure 30 : Schéma conceptuel de l'essai



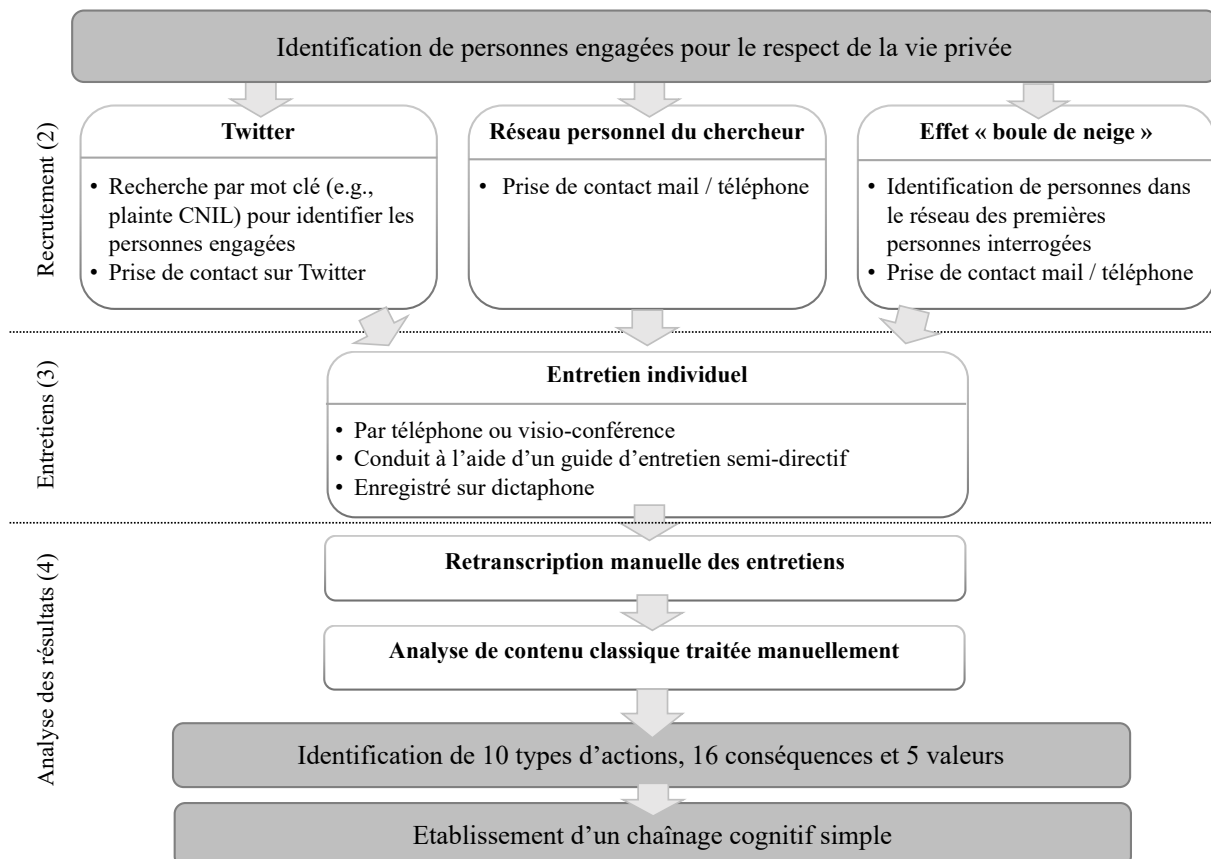
Cela conduit à considérer qu'un droit individuel (de protection des données personnelles) pourrait être construit et développé de manière collective, par la mise en œuvre de pratiques sociales de protection de la vie privée. Ainsi, notre recherche vise à répondre à la question suivante : **Comment des valeurs, structurant des pratiques sociales partagées, peuvent-elles influencer les réponses fondées sur la pratique d'un droit individuel ?**

Section 3. Méthodologie et recherche empirique

Dans cette troisième section, nous détaillons notre approche qualitative adoptée (1), les procédures de recrutement (2) et d'entretiens (3), la méthode d'analyse des résultats (4).

Les grandes étapes de notre méthodologie sont précisées dans la Figure 31 ci-dessous.

Figure 31 : Étapes de la méthodologie



1. Approche qualitative

Notre recherche a pour objectif d'explorer l'influence de normes socio-culturelles sur les actions de protection de la vie privée et face à une violation de données personnelles. Cette question étant encore peu explorée, notre recherche possède une visée exploratoire (Charreire-Petit & Durieux, 2007). Nous avons alors privilégié une approche qualitative, permettant une compréhension globale de l'expérience individuelle et collective.

Nous avons conduit plusieurs entretiens approfondis (N=15) avec différentes personnes actives en matière de protection des données personnelles (soit à titre individuel, soit au sein de collectifs divers) (cf. détail des profils dans le Tableau 36). Ces entretiens étaient semi-directifs. Les entretiens ont été menés par l'auteure entre le 20 décembre 2021 et le 25 février 2022, à distance (téléphone et visio). Ils ont été enregistrés et retranscrits manuellement. Les entretiens ont duré entre 54 minutes et 1h30 (durée moyenne : 1h06 ; durée totale : 16h35), générant un corpus de 253 pages et 151.880 mots.

2. Procédure de recrutement

2.1. Procédure de recrutement

L'objectif premier de notre recherche est d'identifier les principales valeurs motivationnelles en jeu pour les personnes engagées dans le respect du droit à la vie privée. Les personnes interrogées ont été identifiées car elles manifestaient un comportement de protection de la vie privée (social, technique, institutionnel).

Certaines personnes interrogées ont été identifiées et contactées via Twitter car elles interagissent avec d'autres personnes sur le sujet de la protection de la vie privée (elles avaient posté un message identifié par l'auteur à l'aide d'une recherche par mot clé ; par exemple : CNIL). Les autres personnes ont été contactées par un effet de recrutement « boule de neige » ou par relations personnelles. Au final, parmi les 15 personnes interrogées, 8 personnes ont été contactées directement sur Twitter, 3 personnes au sein du réseau direct du chercheur et 4 personnes par un effet « boule de neige ».

Plusieurs difficultés ont été rencontrées au moment du recrutement :

- Les personnes actives pour la protection de leurs données personnelles souhaitent généralement rester anonymes ou sont réticentes à nouer des contacts extérieurs et inconnus ;
- La CNIL a refusé de nous mettre en contact avec des personnes leur ayant déposé une plainte, par souci de protection de leur anonymat ;
- Malgré de nombreuses et insistantes tentatives, nous n'avons pas réussi à obtenir des entretiens avec des associations françaises de protection des consommateurs (UFC Que Choisir et 60 millions de consommateurs).

En synthèse, d'une part, le sujet de la protection des données personnelles des consommateurs est encore très peu développé et d'autre part, les personnes concernées sont très vigilantes sur leur protection. Ces aspects sont à garder à l'esprit pour de futures explorations.

2.2. Questionnaire préalable à l'entretien

Un questionnaire préalable établi sur la plateforme Jotform (<https://www.jotform.com/>) a été transmis par mail avant l'entretien (cf. Annexe 8), afin de valider les trois types de comportements de protection de la vie privée : utilisation d'outils protecteurs, engagements associatifs ou sociaux et dépôts de plaintes à la CNIL. Les résultats sont indiqués dans le Tableau 36 page suivante.

Les questionnaires ont été envoyés par Jotform (<https://www.jotform.com/>). Nous avons oublié de faire figurer sur ce questionnaire des indications concernant le respect de la confidentialité des répondants dans le cadre d'une recherche académique. Le répondant #12 a souligné ce point, que nous gardons bien à l'esprit pour la suite de nos recherches.

Deux premiers phénomènes sont à souligner : (i) trois personnes ont refusé de répondre au questionnaire préalable, dans un souci de limiter le partage de leurs informations personnelles. Les données ont alors été complétées à l'issue de l'entretien pour les trois personnes manquantes ; (ii) aucune des personnes interrogées n'a indiqué avoir engagé une procédure judiciaire.

Les réponses obtenues au questionnaire préalable sont très variables et dépendent fortement de la perception que la personne a de son engagement (ce point sera discuté à la fin de l'essai). Pour exemples :

- (i) le répondant #3 déclare être très peu engagé socialement dans la défense de la vie privée, alors qu'il a fait un choix délibéré de s'orienter professionnellement dans ce secteur (avec un engagement fort en termes de moyens et de formations nécessaires). Ce même répondant met régulièrement des messages sur les réseaux sociaux afin d'éduquer et sensibiliser son entourage professionnel aux pratiques de protection des données personnelles ;
- (ii) le répondant #11 déclare dans le questionnaire faire attention au partage de ces informations personnelles (oui à la question sur l'utilisation d'outils protecteurs), ce qui concrètement s'est traduit lors de l'entretien par ne pas mettre de photos d'enfants sur Facebook ; alors que le répondant #6 affirme ne pas être assez vigilant (non à la question sur l'utilisation d'outils protecteurs), alors que cette personne utilise des logiciels tels que Signal ou Telegram et déploie beaucoup d'efforts pour protéger ses informations personnelles, comme apprendre par cœur les adresses mail de ses contacts.

Ceci confirme le décalage souvent souligné dans la littérature entre comportement déclaré et comportement réel de protection de la vie privée (Pavlou, 2011) et nous incite dans des recherches futures à trianguler nos résultats avec d'autres données (nous précisons ce point dans le paragraphe 4.2.2. portant sur les limites de notre recherche). De fait, nous avons complété certaines réponses obtenues.

Tableau 36 : Profils des personnes interrogées

#	Âge	Profession ou activité	Utilisation d'outils protecteurs	Engagement associatif ou social	Plainte déposée à la CNIL
#1	25-44 ans	Doctorant en économie politique (sujet : société de surveillance)	Oui	Plutôt moyennement engagé dans le milieu associatif	Non
#2	25-44 ans	Professeur (IA & Data)	Oui	Oui, très engagé	Oui
#3	45-64 ans	Avocat, Délégué à la protection des données personnelles	Non	Plutôt moyennement engagé socialement	Non
#4	25-44 ans	Web développeur	Oui	Oui, très engagé	Oui
#5	25-44 ans	Doctorant (CIFRE ANSII ¹⁰⁴)	Oui	Oui, très engagé	Non
#6	25-44 ans	Enseignant-chercheur en sciences de gestion	Oui	Pas du tout engagé	Non
#7	25-44 ans	Ingénieur IT	Oui	Oui, très engagé	Oui
#8	25-44 ans	Ingénieur IT	Oui	Oui, très engagé	Oui
#9	25-44 ans	Support IT	Oui	Oui, très engagé	Oui
#10	25-44 ans	Boulangier en reconversion	Oui	Pas du tout engagé	Non
#11	25-44 ans	Manager en banque - finance	Oui	Pas du tout engagé	Non
#12	45-64 ans	Enseignant-chercheur en pharmacie et biochimie	Oui	Pas du tout engagé	Non
#13	45-64 ans	Travailleur social	Oui	Oui, très engagé	Non
#14	25-44 ans	Chef de projet en IA	Oui	Pas du tout engagé	Non
#15	25-44 ans	Vendeur de matériel informatique	Oui	Pas du tout engagé	Non

Nota bene : les citations ci-après sont attribuées à leur auteur par son numéro (par exemple, le premier répondant est indiqué #1).

¹⁰⁴ Agence Nationale de la Sécurité des Systèmes d'Information.

3. Procédure d'entretiens

Les entretiens ont été menés en français. Le guide d'entretien utilisé est présenté en Annexe 9.

Les entretiens se sont déroulés en ligne, selon le moyen préféré par la personne interrogée : soit par vidéo avec caméra, soit par vidéo sans caméra, soit par téléphone. Une personne interrogée ne nous a jamais communiqué son prénom et reste à ce jour totalement inconnue.

Les entretiens ont débuté par une présentation et quelques minutes de discussion conviviale. Le guide d'entretien est ensuite composé de 4 parties :

- Une première série de questions portant sur les comportements de protection de la vie privée : d'abord ceux liés à la raison pour laquelle la personne interrogée a été contactée, puis l'analyse des autres types de comportements. Ces questions permettent de valider et de comprendre les comportements constatés et déclarés préalablement à l'entretien, et de les compléter. Nous avons repris la classification en trois catégories proposées dans cette thèse : réponses sociales, réponses techniques et réponses institutionnelles (bien comprises par les répondants) ;
- Une deuxième série de questions sont posées pour comprendre le rôle joué au sein du groupe social : conscience de son rôle et reconnaissance par les autres membres du groupe (les parties 1 et 2 peuvent être inversées selon les répondants) ;
- Au fur et à mesure de l'échange, des questions sont posées pour mieux comprendre les motivations à adopter ces comportements favorables à la protection de la vie privée, l'objectif principal de l'entretien étant de comprendre le chaînage cognitif du répondant. Ceci nous aide à progresser vers une abstraction des motivations et des valeurs terminales. Une série de questions plus dirigées, reposant sur la question « pourquoi est-ce important pour vous » (Reynolds & Gutman, 1988), nous permettent d'approfondir les motivations profondes. Lorsque la personne rencontre des difficultés à répondre, les techniques de projection de la « troisième personne sondée » proposées par Reynolds et Gutman (1988) sont utilisées (i.e., demander au répondant de décrire mentalement une personne active pour la protection des données personnelles et ses motivations pour cela). Cette technique a été assez bien perçue par les répondants ;
- Enfin dans une quatrième et dernière partie, nous interrogeons les personnes sur leurs réactions en cas de piratage de la Caisse Nationale d'Assurance Maladie (CNAM). Nous avons choisi ce scénario de piratage informatique de la CNAM pour son côté

catastrophique, proches des cyberattaques de centres de santé et hospitaliers. Si ces cyberattaques sont de plus en plus fréquentes (en 2021, en moyenne, un incident par semaine intervient dans une entité du secteur de la santé¹⁰⁵), elles ont été surtout médiatisées avec la cyberattaque du centre hospitalier de Corbeil-Essonnes fin août 2022, c'est-à-dire après les entretiens avec les répondants. Au moment des échanges, une cyberattaque de la CNAM reste encore hypothétique pour les répondants, et nous n'avons pas eu le sentiment que les répondants étaient majoritairement conscients de l'ampleur des attaques des centres de santé et des risques encourus.

Les entretiens se sont globalement très bien déroulés. Ils ont offert de belles rencontres et plusieurs personnes interrogées nous ont envoyé des messages de remerciements après les entretiens (« Merci pour cet échange qui m'aura permis de m'interroger sur mes motivations profondes (et de continuer à m'interroger sur ce sujet). J'en sors grandi et nourri ! », « J'ai été extrêmement ravie ! », « Bon courage pour la suite, c'est un sujet intéressant »).

Les entretiens ont été retranscrits manuellement : majoritairement par une personne externe à l'étude (aide amicale fournie) et dans une très moindre mesure par l'auteure. Ceci nous permet de disposer d'un corpus de 253 pages, travaillé selon la méthode d'analyse que nous précisons dans le paragraphe suivant.

¹⁰⁵ <https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/portraits-de-la-relance/centre-hospitalier-universitaire-de-reims/>

4. Méthode d'analyse

Cet essai nécessite de préciser plusieurs points méthodologiques. C'est pourquoi dans ce paragraphe nous établissons une comparaison des méthodes d'analyse envisagées (4.1.), aboutissant à la méthode de chaînage cognitif classique adoptée (4.2.). Nous analysons également la pertinence de notre travail au regard de la théorie de la pratique (4.3.).

4.1. Comparaison des méthodes d'analyse envisagées

Notre objectif initial dans le cadre de notre thèse de doctorat était d'adopter une méthodologie de chaînes « Moyens-Fins » (Reynolds & Gutman, 1988). Pour cela, notre questionnaire intègre à plusieurs reprises la question « Pourquoi est-ce important pour vous ? ». Cependant, les entretiens ont fait apparaître de nombreux aspects que nous n'avions pas envisagés (e.g., l'importance des dynamiques collectives, le rôle des pratiques sociales). De plus, nous avons été interrogés pendant la pré-soutenance sur la consistance d'une analyse par les chaînes Moyens-Fins, compte tenu du nombre faible d'observations. Nous nous sommes donc beaucoup interrogés sur l'approche méthodologique à apporter à l'analyse. Dans le cadre du présent manuscrit, il nous paraît pertinent de consacrer une partie à ces réflexions méthodologiques. Chacune des trois techniques seront détaillées ci-après : (i) analyse thématique classique, (ii) chaînes Moyens-Fins, (iii) analyse textuelle automatique. Nous concluons sur une partie justifiant la méthode utilisée.

4.1.1. Méthode 1 : analyse thématique de contenu classique

L'analyse thématique de contenu est une opération qui consiste à donner du sens à un texte multiforme et varié, i.e., à transformer un ensemble empirique en éléments théoriques. Cette analyse de contenu consiste à découper les données (e.g., retranscriptions d'entretiens) en codes ou unités d'analyse puis à regrouper ces codes au sein de catégories et méta-catégories. Les codes peuvent reposer sur des fondements théoriques ou non. Ainsi, le chercheur établit une grille d'analyse fondée sur les catégories définies permettant de structurer les observations et de produire du sens (Allard-Poési, 2003).

Afin d'être en capacité d'extraire un cadre théorique original et d'éviter tout risque de circularité, une première étape est conseillée : l'attention flottante (Dumez, 2021), i.e., une

capacité à considérer un corpus ou un matériau dans son entièreté : on lit tout, on ne prend aucune note, on laisse son esprit divaguer.

4.1.2. *Méthode 2 : chaînes Moyens-Fins*

La méthode des chaînes Moyens-Fins (Gutman, 1982; Reynolds & Gutman, 1988) est basée sur une question centrale : « Pourquoi est-ce important pour vous ? », permettant de réassembler la hiérarchie perceptive reliant les attributs d'un produit (i.e., caractéristiques incontournables permettant de décrire un produit) aux conséquences (i.e., qui dérivent de l'usage du produit) et valeurs associées (Rokeach, 1973). L'analyse des chaînes moyens-fins a beaucoup été mobilisée en marketing afin de mieux comprendre les structures cognitives associées à l'achat d'un produit ou d'un service, de mettre en relation l'acte de consommation et les sensibilités principales (i.e., les chaînages) et d'éclairer les questions de consommation de produits, de segmentation et de ciblage publicitaire.

Les chaînages Moyens-Fins s'appuient sur trois techniques (Valette-Florence, 1994) :

- la méthode originelle par entretien semi-directif (Reynolds & Gutman, 1988), qui consiste à partir d'un « point d'ancrage », i.e., un produit choisi, à interroger successivement les individus pour les faire passer petit à petit à un niveau d'abstraction et jusqu'à ce qu'une valeur terminale soit citée ;
- les méthodes de protocole écrits, basées sur des questionnaires (Walker & Olson, 1991) ;
- les entretiens par carte, mobilisant des entretiens de groupe (Valette-Florence & Rapacchi, 1991).

Dans le premier cas, et selon notre compréhension, la totalité du processus cognitif peut être couverte à partir d'une cinquantaine d'entretiens semi-directifs (d'une durée de 30 à 60 minutes) lorsque plusieurs chaînes sont citées par un même individu (Valette-Florence, 1994).

Cependant, une quinzaine d'entretiens suffisent pour avoir un premier chaînage cognitif (Aurifeille, 1993) et générer une première liste des différents niveaux, qui peuvent par la suite être utilisés à plus grande échelle : notre recherche s'inscrit dans cette logique.

Enfin il existe trois grandes méthodes d'analyse des résultats, dont l'objectif est de segmenter les consommateurs (pour des stratégies de communication ou de positionnement) :

- l'analyse causale et la détermination des chaînages latents (ou abstraits) ;
- la méthode basée sur la construction de cartes hiérarchiques, i.e., des représentations graphiques planes et agrégées des différentes chaînes évoquées par les répondants ;
- la méthode des chaînes virtuelles.

4.1.3. Méthode 3 : analyse textuelle automatique

Une troisième méthode consiste dans le traitement automatique et statistique de corpus de textes important. Ces méthodes portent un fort intérêt de par les volumes de texte numérisés et facilement accessibles et les outils de traitement existants. « Si une analyse thématique manuelle est possible sur un corpus limité (une trentaine d'entretiens par exemple), l'analyse automatique vient au secours pour un grand nombre de documents » (Balech & Benavent, 2019, p.4). Sans qu'aucun seuil ne semble réellement défini, ces analyses sont essentiellement mobilisées sur les corpus de textes importants.

Plusieurs outils permettent des analyses textuelles automatiques (e.g., Iramuteq¹⁰⁶, R.Temis ou package « themis » sur r, cleanNPL), qui reposent sur les langages R et Python. Ces techniques d'analyse de données textuelles font appel à la statistique et à l'ingénierie linguistique (Moscarola, 2018). Elles permettent ainsi des analyses factorielles de correspondances. Le principe est le même que pour le traitement de questionnaires à variables qualitatives.

Enfin ces analyses nécessitent une certaine vigilance et peuvent parfois faire apparaître des résultats étonnants. Par exemple : « le mot « ennui » n'apparaît que 7 fois dans Madame Bovary alors que l'« idée » d'ennui, elle, y est omniprésente » (Carbou, 2017, p.6).

¹⁰⁶ <http://www.iramuteq.org>

4.1.4. Comparatif des méthodes

À l'aide de l'analyse précédente, nous présentons dans le Tableau 37 ci-dessous une analyse comparative des différentes méthodes. Il apparaît clairement que le corpus de données obtenu n'est pas suffisant pour conduire soit une analyse de chaînes Moyens-Fins soit une analyse textuelle automatique. De plus, les analyses textuelles automatiques (fort intéressantes) demandent une certaine maîtrise et expérience. Enfin, plusieurs aspects sont apparus en dehors de l'analyse (comme l'approche structurelle de la théorie de la pratique), plus facilement traitable par une analyse de contenu classique.

Nous avons donc décidé de procéder à un chaînage cognitif simple (méthode originelle de Reynolds & Gutman (1988) précédé d'une analyse de contenu classique traitée manuellement (avec le support du logiciel NVivo 11). Nous les expliquons dans le paragraphe suivant.

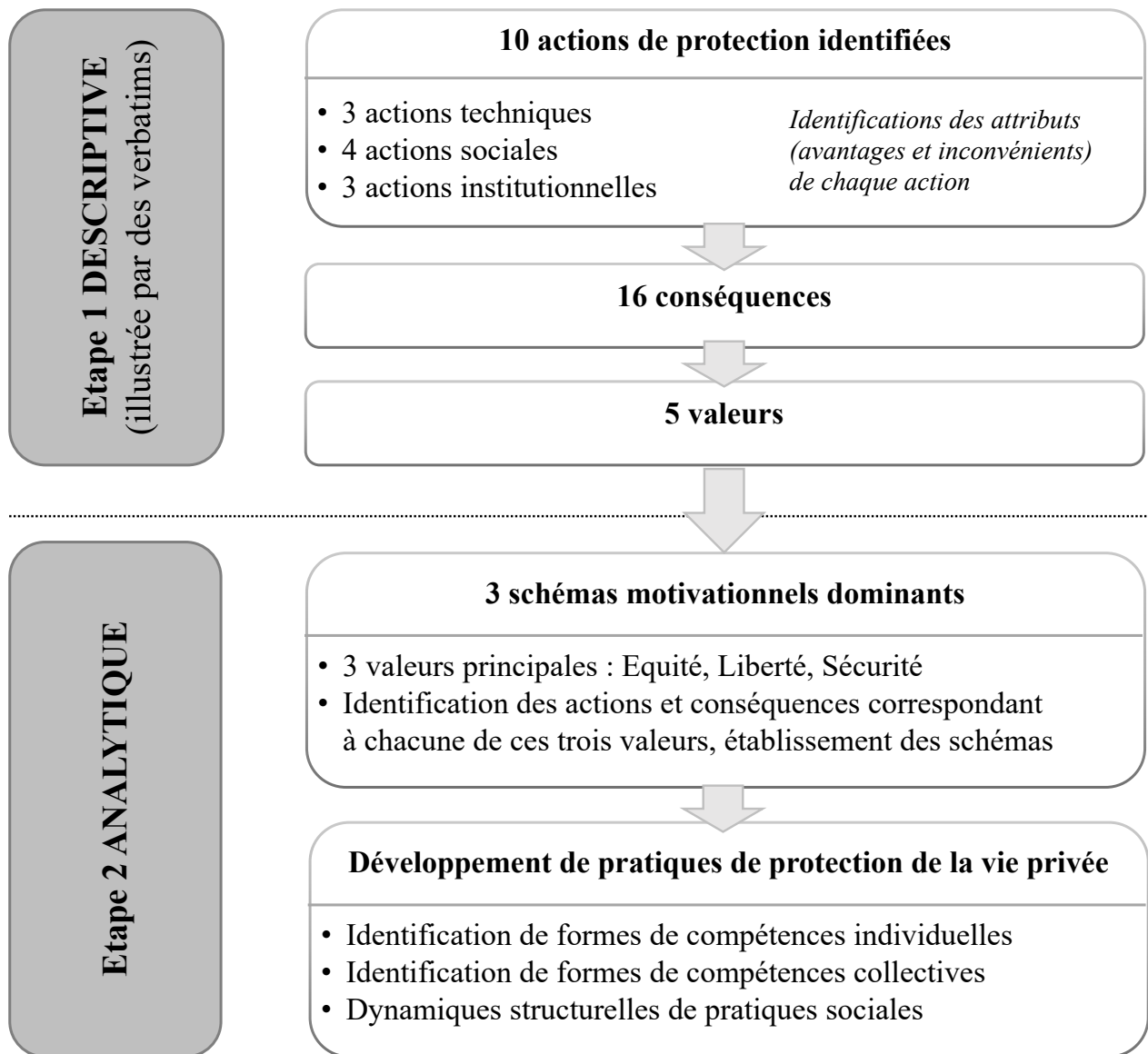
Tableau 37 : Tableau comparatif des méthodes

Méthode	Avantages	Inconvénients
Analyse de contenu classique	- Richesse du contenu - Analyse en profondeur	- Lourdeur de l'analyse - Manque de représentativité
Chaînes moyens-fins	- Richesse du contenu - Identification claire des motivations d'achat	- Difficultés à distinguer les chaînages réellement cités par le répondant et l'interprétation du chercheur
Analyse de contenu automatique	- Richesse des volumes de données exploités - Richesse des analyses	- Besoin de maîtrise de R et Python - Ne remplace pas le regard

4.2. Procédure d'analyse choisie

Notre analyse a procédé en deux grandes étapes, que nous présentons sur la Figure 32 ci-dessous : une première étape descriptive, au cours de laquelle nous avons identifié les codes et catégories de notre analyse que nous présentons dans cette partie (4.2.1), faisant quelques choix sémantiques ; puis une deuxième partie plus analytique, au cours de laquelle nous établissons les schémas motivationnels et identifions les trois schémas principaux (4.2.3), puis nous analysons les pratiques de protection de la vie privée (4.2.4).

Figure 32 : Schéma général de présentation des résultats



4.2.1. *Analyse de contenu et établissement des codes*

Nous avons structuré le corpus en catégories basées sur des codes (Allard-Poési, 2003). Les codes ont ainsi été revus et regroupés au fur et à mesure, entre mars et octobre 2022, manuellement et à l'aide du logiciel NVivo11. Les données ont été classées en 5 catégories :

- Les codes pour les réponses de protection (sociales, techniques et institutionnelles),
- Les codes pour les réponses face à une violation de données personnelles,
- Les codes pour les conséquences des réponses de protection,
- Les codes pour les valeurs socio-culturelles dominantes,
- Les codes pour les formes de compétences individuelles ou collectives.

Nous aboutissons à la définition de 10 types d'actions, 16 conséquences et 5 valeurs. En particulier, les valeurs sont définies telles que citées par les individus, sans faire nécessairement appel à des valeurs préétablies (Valette-Florence, 1994).

4.2.2. *Méthode de chaînage cognitif*

La méthode de chaînage cognitif (Reynolds & Gutman, 1988; Valette-Florence, 1994; Valette-Florence et al., 2003) a été utilisée pour établir les schémas motivationnels culturels. De façon classique, il s'agit d'établir des relations entre des attributs (i.e., caractéristiques incontournables qui permettent de décrire un produit), des conséquences (i.e., qui dérivent de l'usage du produit) et des valeurs associés. Pour cela, ces relations sont citées par le répondant lors de l'entretien semi-directif, reposant essentiellement sur la question : « pourquoi est-ce important pour vous ? ». Le chercheur cherche également à établir des relations lors du codage des données.

Dans notre contexte, le schéma motivationnel consiste à établir un lien entre une action de protection de la vie privée (techniques, sociales, institutionnelle), des conséquences (e.g., limiter le SPAM) et des valeurs associées (idéaux). La difficulté a résidé dans la définition des attributs pour les actions de protection de la vie privée. Nous avons fait le choix de définir comme attribut les réponses de protection, correspondant ainsi à la caractéristique permettant de la décrire (e.g., démultiplier les services). Les conséquences dérivent alors de l'usage de ces réponses.

Les entretiens ayant été longs (durée moyenne = 1h06) et riches, les répondants se sont prononcés sur leurs motivations concernant différentes actions, sociales, techniques ou institutionnelles. Ainsi, nous obtenons au total 95 chaînes (ou *ladders*) avec une moyenne de 6.3 chaînes par répondant. Compte tenu de ce nombre conséquent de chaînes, ces données ont été saisies dans le logiciel de saisie LadderUX¹⁰⁷ pour nous aider dans le traitement et la visualisation des résultats. Cependant le nombre d'entretiens reste insuffisant pour conduire une analyse de chaînes Moyens-Fins consolidée, nous ne précisons pas les résultats obtenus (non significatifs) et nous indiquons la matrice d'implication et la carte hiérarchique à titre d'illustration en annexes (respectivement Annexe 11 et Annexe 12).

Sur cette base, nous avons isolé les trois schémas motivationnels dominants, i.e., avec les fréquences de citations les plus importantes.

¹⁰⁷ <https://ladderux.org/>

4.2.3. *Analyse des pratiques sociales de protection de la vie privée*

Dans ce dernier paragraphe de la partie méthodologique, nous souhaitons préciser l'approche épistémologique et méthodologique de la compréhension d'une pratique sociale de la protection de la vie privée. En effet, notre approche à travers des entretiens semi-directifs est centrée sur l'individu (agent) et moins sur la pratique sociale en elle-même (Bourdieu, 1972).

D'autres études s'appuyant sur la théorie de la pratique reposent également essentiellement sur des entretiens (collectifs ou individuels). Par exemple, Shove & Pantzar (2005) expliquent comme la pratique de la marche nordique se développe dans des pays divers le Japon, la Norvège et les États-Unis, en se basant sur des entretiens individuels, la participation à une marche et quelques groupes de discussion (cet article montre que cette pratique sportive se développe par un processus d'intégration successive d'images, d'artefacts et de formes de compétences, par les consommateurs et qui est localisé). Lunnay et al. (2011) étudient les pratiques de consommation d'alcool chez les adolescentes australiennes sur la base de groupes de discussion et d'entretiens individuels (au cours desquels les jeunes filles présentent quelques photos de leurs occasions de consommation d'alcool ; permettant une petite triangulation des données).

De plus, l'approche qui consiste à observer « ce que les gens font effectivement » (*what people actually do*) en les interrogeant est assez classique : elle réside sur le principe d'individuation des actions. L'action est liée alors à l'intention de l'acteur (Davidson, 1980). L'action individuelle est représentative de la structure sociale car les structures sociales contraignent l'action individuelle (Giddens, 1984).

En conclusion, notre démarche basée uniquement sur des entretiens individuels nous semble suffire pour constituer une approche des pratiques de protection des données personnelles. Ensuite et au cours de la vie de cette recherche, il pourra être intéressant de compléter avec d'autres sources de données.

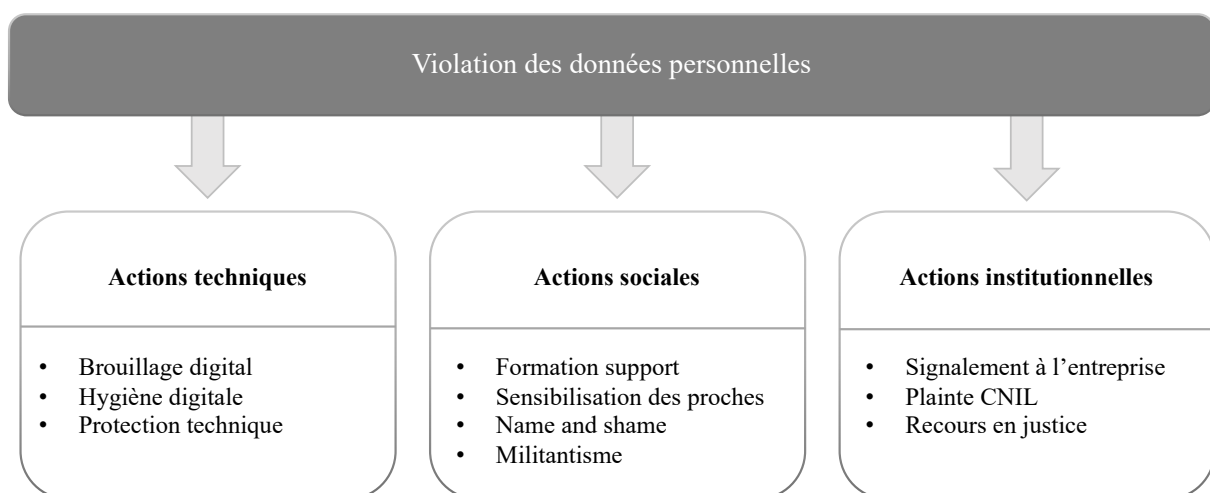
Section 4. Résultats descriptifs de la recherche

Conformément à l'approche montrée dans la Figure 32, et pour plus de clarté, nous distinguons les résultats descriptifs (ci-après) de notre recherche et les résultats analytiques (dans la section 5). Dans cette partie, nous présentons dans un premier paragraphe une typologie actualisée des actions de protection de la vie privée (1), puis les conséquences et les valeurs identifiées (2) qui seront ensuite mobilisées et que nous illustrons avec des verbatims.

1. Actions de protection de la vie privée

Comme nous l'avons précédemment évoqué, nous proposons dans le cadre de cette thèse de doctorat une typologie des réponses de protection des données personnelles issue de la typologie de Son & Kim (2008) et organisée en trois blocs : les actions techniques, les actions sociales et les actions institutionnelles. Les entretiens conduits dans le cadre de cette recherche ont été l'occasion de valider et de compléter cette typologie (sans visée conceptuelle approfondie). Cette organisation en trois blocs a été bien comprise et acceptée par l'ensemble des répondants : nous pouvons en conclure qu'elle peut être gardée la suite de notre analyse. Nous proposons donc ci-après de reprendre chaque type d'actions, de les compléter et les modifier quand cela est nécessaire : les actions techniques (1.1.), les actions sociales (1.2.), que notre approche méso a particulièrement permis d'enrichir, et les actions institutionnelles (1.3.) L'ensemble des actions (décrites et illustrées par la suite) sont reprises dans la nouvelle classification ci-dessous Figure 33 :

Figure 33 : Actions de protection des données personnelles



De plus, les personnes ont été interrogées sur leurs comportements de protection de la vie privée de façon générale et face à une violation conséquente de leurs données personnelles en particulier : nous indiquons alors à la fin de ce paragraphe dans quelle mesure ces actions se reproduisent ou se différencient dans le cas d'une violation de données personnelles.

Enfin, pour chaque type d'actions, nous précisons leurs attributs (avantages et inconvénients spécifiques à chaque action) : cela nous permet d'identifier les actions opérationnelles envisageables à améliorer que nous proposons à la fin de cet essai.

1.1. Actions techniques

Nous avons initialement identifié trois actions techniques (cf. Figure 27) : (i) applications de mesure de sécurité informatique, (ii) falsification des informations, (iii) application des droits de retrait et d'effacement. Par rapport à cette catégorisation :

- Nous renommons « applications de mesure de sécurité informatique » plus simplement en « protection technique » ;
- Nous incluons « falsification d'informations » dans une catégorie plus large nommée « brouillage digital » ;
- Nous excluons l'application des droits de retrait et d'effacement des actions techniques, qui est comprise par les répondants comme une action institutionnelle (cf. p. 45) ;
- Nous ajoutons une catégorie « hygiène digitale ».

Nous précisons chacune de ces actions ci-après et les reprenons dans le Tableau 38.

1.1.1. Protection technique

La première catégorie : « **Protection technique** » inclut les applications de sécurité informatique précédemment citées (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018) et toute une série d'usages d'outils spécifiques : portant sur le matériel (choix des terminaux et des systèmes d'exploitation), sur le mode de transfert des données (e.g., chiffrement des communications), sur le blocage des outils de tracking publicitaire (e.g., Blocktel), sur l'usage d'applications spécifiques (e.g., Freetube). Nos résultats suggèrent que ces usages de protection technique sont soit des choix individuels ou soit l'utilisation de moyens mis à disposition par l'employeur.

1.1.2. Brouillage digital

Deuxièmement, les répondants font souvent part d'un usage : la démultiplication des services, i.e., l'usage de nombreuses adresses e-mail et de nombreux comptes. Il s'agit d'une technique utilisée par tous les répondants, et les répondants peu à l'aise avec la technique y consacrent beaucoup de temps et d'énergie. Plusieurs répondants parlent d'une technique de partage des comptes (e.g., Netflix, Spotify) non seulement dans un objectif économique (partage des frais d'abonnement entre plusieurs ménages) mais également dans un objectif de rendre difficile, voire impossible, la construction de profils et de *personae*. Ainsi, ces différentes techniques répondent à un objectif commun de « brouiller les pistes ». Il s'agit du même objectif que la falsification d'informations, nous les regroupons dans une catégorie : « **Brouillage digital** ».

1.1.3. Hygiène digitale

La catégorie « **Hygiène digitale** » consiste à faire le ménage après tout usage et à nettoyer les différentes traces laissées derrière soi : indications GPS et connexions Bluetooth, limiter les documents laissés sur le cloud, nettoyer les accès aux comptes, les cookies, les corbeilles. Nous incluons dans cette catégorie l'usage limité des réseaux sociaux (même objectif de laisser le moins de traces et de données personnelles).

Tableau 38 : Détail des réponses techniques

Types de réponses techniques	Détails des réponses	Verbatims illustratifs
Brouillage digital	Démultiplier les services	« pour moi la bonne pratique (...) c'est de ne pas utiliser un service pour tout faire (...) c'est démultiplier les services pour démultiplier les actions. c'est toutes ces bonnes pratiques (...) qui (...) au-delà des outils, sont clefs » (#2)
	Falsifier les informations	
	Partager les comptes	
Hygiène digitale	Couper GPS et Bluetooth	« Je pense que je prête attention à réduire mes traces. Pas forcément à les faire disparaître, mais juste être attentif au quotidien, ce que j'appelle un peu d'hygiène numérique et d'essayer éviter de laisser des traces de partout » (#9)
	Limiter ce qui est sur le cloud	
	Nettoyer les cookies, les accès aux comptes, les corbeilles	
	Ne pas publier sur les réseaux sociaux	« je suis pas mal absent de tout ce qui est réseaux sociaux (...) parce qu'effectivement, les réseaux sociaux, c'est, une grosse partie (de) nos données personnelles » (#15)
Protection technique	Matériel : Choix des terminaux et des systèmes d'exploitation	« Dans vos usages personnels, est-ce que vous faites attention au navigateur que vous utilisez ? (...) Pas du tout. Après, j'utilise des moyens, des outils informatiques qui sont mis à disposition par mon employeur. J'ai que mon ordinateur pro. J'ai un téléphone pro avec double SIM » (#11)
	Mode de transfert de données : chiffrement des communications, choix des clouds spécifiques (ex. Dropbox), usage de VPN, protection des mots de passe	
	Blocage de publicité : Blocktel Utilisation d'adblockers spécifiques	« il y a (...) des blockers qui sont simples, (...) efficaces, qui fonctionnent bien, que ce soit des adblockers, des bloqueurs de cookies ou des bloqueurs de systèmes » (#2)
	Freetube, navigateurs spécifiques	

1.1.4. *Avantages et inconvénients des réponses techniques*

Les répondants citent ces pratiques techniques comme étant **complexes et laborieuses**. Cette complexité repose sur 5 facteurs (cf. Tableau 39) : (i) performance des outils, (ii) connaissance technique nécessaire, (iii) blocage de la langue, (iv) complexité d'utilisation, (v) coût perçu. Tout d'abord, les outils ne sont pas performants soit parce qu'ils nécessitent des connaissances techniques, soit parce qu'ils ne sont pas bien configurés (e.g., Blocktel qui ne bloque pas la prospection commerciale depuis des centres d'appels basés à l'étranger). D'autre part, l'utilisation est de fait complexe car elle demande du temps et de la discipline. Enfin, ces différents attributs sont liés entre eux : la connaissance technique rend tout usage protecteur beaucoup plus lent à mettre en place. Par exemple, les individus consacrent beaucoup de temps et d'énergie à essayer de se protéger (par exemple, une répondante essaie d'apprendre par cœur toutes les adresses e-mails de ses contacts), alors que l'utilisation d'une messagerie cryptée sera plus protectrice et moins contraignante.

Tableau 39 : Avantages et inconvénients des réponses techniques possibles

Attributs	Verbatims illustratifs
1. Manque d'outils performants	« il nous manque des outils (...) Ils existent, mais ils ne fonctionnent pas très bien. Par exemple, BigBlueButton (..) j'ai du mal à le recommander (...) Moi, je vais savoir le configurer (..) mais une personne lambda, ben ça marche pas (...) » (#8) « je vais déjà utiliser les services que l'Etat propose (...Blocktel) Ca marche plus ou moins (...) quand quelqu'un nous appelle quand même de l'étranger, pour dénoncer le numéro, il y a une procédure qui est (..) assez complexe» (#10)
2. Nécessité d'avoir des connaissances techniques	« Pourquoi les gens utilisent Apple majoritairement ? Parce que tu allumes l'ordi, c'est prêt, point. C'est ça. Pourquoi les gens n'utilisent pas Linux, que Linux, techniquement, ça pourrait être la plateforme la plus sécurisée, parce que Linux, si on n'a pas envie d'un peu s'intéresser à installer un programme, ben, ce n'est pas facile d'utilisation, en fait » (#14)
3. Blocage de la langue	« C'est pas toujours évident de comprendre et si en plus vous trouvez des ressources en anglais, c'est encore pire (...), comprendre l'anglais, c'est une chose, mais comprendre l'anglais technique, c'est encore autre chose » (#10).
4. Complexité d'utilisation	« Ça me semble compliqué de m'assurer qu'il y ait plein d'accès qui soient fermés. (...) mais aussi indispensable si je veux être sûre que c'est moi qui y ai accès et pas quelqu'un d'autre (...) c'est laborieux techniquement » (#6) « cette idée de démultiplier (...) les outils, parce qu'il n'y a aucun outil qui, du coup, est packagé, et qui permet de tout faire en même temps. (...) en fait, ça demande un effort ; ça demande une discipline» (#2) « J'ai abandonné parce je trouve, en fait, que ce n'est pas du tout pratique. » (#3)
5. Coût perçu	« Mais qu'est-ce qui te manque pour passer à l'étape suivante ? (...) peut-être un peu d'argent, parce que j'ai l'impression que des outils supplémentaires, ils sont payants. Un bon VPN, qui marche correctement, c'est un abonnement. » (#6)

Nota bene : L'action technique « tout couper » n'avait pas été incluse. Cette action a été abordée avec un seul répondant, qui ne l'a pas pratiquée lui-même : elle ne peut donc pas être retenue comme une option. *« J'ai lu pas mal d'expériences (...) de journalistes ou d'acteurs de l'écosystème qui avaient fait cette démarche comme (...) couper son compte Google et compagnie (...) définitivement. Et en fait, on se rend compte (...) ce sont des systèmes et des services qui font partie de nos vies et (...) il y a plein de solutions alternatives qui existent, mais qui ne sont pas autant déployées et autant interopérables avec tout ce qui existe aujourd'hui et qui nous forcent un petit peu à contourner tout le temps les systèmes (...) C'est clair qu'à un moment donné, pour faciliter l'accès à l'intercommunication avec des collègues, avec des proches, et ben en fait, c'est très limitant. » (#2)*

1.2. Actions sociales

Nous avons précédemment identifié deux actions sociales (cf. Figure 27) : (i) le bouche-à-oreille négatif et (ii) le e-WOM (word-of-mouth), qui en réalité sont proches et pourraient être regroupées. De ce fait, il est impératif de mieux préciser les actions sociales possibles. Ceci est possible grâce à notre recherche conduite à un niveau méso, permettant ainsi de s'interroger sur les dynamiques des groupes. Nous reprenons totalement la classification des actions sociales et distinguons : les formations support (1.2.1.), la sensibilisation des proches (1.2.2.), le « name and shame » (1.2.3.) et le militantisme (1.2.4.).

1.2.1. Formation support

Précisons une première catégorie non citée auparavant, celle de la « **Formation support** » (cf. Tableau 40). La formation support est importante pour la prise de conscience des risques liés à la protection des données personnelles. Plusieurs personnes ont cité des formations suivies par des représentants de l'ANSII dans des parcours universitaires, ayant alors été le déclencheur d'une prise de conscience, ou des formations suivies dans un cadre professionnel. La catégorie « formation support » regroupe tout type d'activités suivies ou pilotées : ateliers de formation au RGPD, ateliers de support d'usage informatique (e.g., pour des personnes âgées isolées techniquement et de fait des services publics).

1.2.2. Sensibilisation des proches

Une deuxième catégorie d'action sociale est la « **Sensibilisation des proches** », qui se rapproche du « bouche-à-oreille » précédemment énoncé, mais qui a un objectif plus large d'informer et de sensibiliser aux risques liés à la protection des données personnelles. Nous observons alors deux comportements diamétralement opposés : soit des personnes décidées à toujours en parler et à faire changer les usages (e.g., tous les membres de la famille et les colocataires d'un répondant ont quitté WhatsApp pour Signal), quitte à être perçues comme trop insistantes, soit des personnes qui préfèrent se taire par peur d'être marginalisées. Ce comportement a été observé par la CNIL auprès des plaignants interrogés (cf. Annexe 10).

1.2.3. Name and shame

Nous avons nommé une troisième catégorie : « **Name and shame** », qui se rapproche du « e-WOM » précédemment énoncé et qui a pour objectif de relayer des informations sur les réseaux sociaux (essentiellement Twitter) pour faire connaître les entreprises peu respectueuses de la protection de la vie privée et des données personnelles, et qu'elles soient ainsi pénalisées.

1.2.4. Militantisme

Une dernière catégorie appelée « **Militantisme** » regroupe l'ensemble des actions militantes ou politiques en vue d'agir pour un plus grand respect de la protection des données personnelles. Ces actions peuvent être locales, notamment à travers les problématiques de l'usage des données dans le développement urbain (e.g., Lyon Urban Data), ou nationales, des collectifs de réflexion techno-critique (e.g., Le Mouton numérique) ou plus largement sur des questions sociétales et écologiques (e.g., Le Mouvement Colibri) et enfin des collectifs plus engagés politiquement (e.g., La Quadrature du Net, dont nous n'avons interrogé aucun membre).

Tableau 40 : Illustrations des actions sociales

Types de réponses sociales	Verbatims illustratifs
Formation et support	« Quand on comprend un minimum de langage, on se sent (...) de plus en plus fort. Et je fais un blog d'ailleurs pour accompagner des débutants » (#13) « Ce que ça veut dire, c'est qu'en gros, quand il y avait une problématique technique un peu pointue, c'était à moi d'aller trouver la réponse précise et d'en faire quelque chose qui soit compréhensible par des gens qui ne sont pas nécessairement des techniciens » (#7) « Je faisais par contre des ateliers de sensibilisation RGPD » (#9)
Sensibilisation des proches	« C'est vrai que j'en parle beaucoup autour de moi et je me suis toujours posé la question « Pourquoi les gens ne sont pas plus avertis des risques et de cette surveillance ? ». Donc j'essaie toujours de faire un travail de sensibilisation » (#5) « Il faut acculturer parce que les gens ne savent pas (...) si les gens savent, (...) peut-être qu'ils prendraient d'autres décisions qu'ils n'en prennent » (#14)
Name and shame	« Plus on en parlera, plus ça se saura, plus on aura des chances que ce sujet soit pris au sérieux, plus il y aura des sanctions et donc plus les entreprises feront attention. C'est la chaîne » (#3) « Le recours, plus exactement, je l'ai publié sur Twitter parce que voilà, j'estime que c'est un sujet d'intérêt public (...) le service public qui, normalement doit être, doit pouvoir être comptable de ses actes auprès du public » (#7)
Actions militantes	« je fais partie d'associations plus locales (... j'ai) une action politique (dans l'objectif) d'amener une population à faire des changements pour aller vers un mieux-vivre ensemble » (#9) « l'engagement associatif (...) c'est la partie plus politique, en gros. C'est le travail collectif, la réflexion collective » (#1) « c'est l'idée d'une action, euh, d'une action collective et partagée, dans le sens qu'elle est construite ensemble » (#1) « aspect de réflexion collective, (et...) produit d'un travail collectif (...) collectif techno-critique » (#1)

1.2.5. Caractéristiques des réponses sociales

Les actions sociales se caractérisent par deux facteurs (ou attributs) :

- La prise de conscience. Les personnes développent des actions sociales parce qu'elles ont conscience des risques liés à la violation de données personnelles et qu'elles veulent les partager (cf. Tableau 41). Et ces actions sociales permettent de développer cette même prise de conscience. Cette prise de conscience peut être comprise comme une distance psychologique avec les risques de violations de données personnelles, i.e., la façon dont un individu est en capacité de se représenter mentalement le phénomène de violation (Trope & Liberman, 2010) est centrale aux actions sociales ;
- La pédagogie et l'empathie dont l'émetteur de ces actions sociales doit faire preuve.

Tableau 41 : Illustrations des réponses sociales

Attributs	Verbatims illustratifs
1. Sensibilité aux risques	« Les personnes qui ont fondé ce genre de milieux avaient des modèles de menaces qui étaient déjà très très avancés (...) on parle de personnes qui ont été en Syrie, qui ont participé aux événements des Printemps arabes (...) qui étaient sur des pays en guerre avec des dictatures, des défenses de dictatures avec MSF, RSF¹⁰⁸. (...) les personnes étaient déjà un peu sensibilisées à ce genre de choses (...) par leurs activités personnelles ou associatives, qui a vu que ça commençait à arriver » (#8) « J'ai été bercé par des récits. Moi, je suis polonais d'origine (...) Donc le bloc de l'Est, tout ça, la police politique, ce genre de choses, c'est des récits que j'ai pas mal entendus dans mon enfance, etc. Forcément, je suis plus allergique que ça à ces choses-là, quoi » (#7)
2. Compétences pédagogiques et empathie	« Quand on est intervenu dans les collèges ou les lycées où ils ont une approche de la vie privée qui est complètement différente de celle qu'on a pu avoir (...) Des choses que nous considérons comme (...) privées, eux, ils s'en foutent complètement. Les profs indiquaient que quand ils confisquaient des téléphones mobiles, ils étaient juste effarés de voir les échanges de contenus entre les élèves, quoi. Il y a des trucs qu'on n'aurait même pas faits à 21 ans et ils le font à 12 ans aujourd'hui, quoi. Et les nude ou les choses comme ça, ça ne les choque absolument plus » (#8) « Au quotidien, je n'essaie pas forcément de faire du prosélytisme, mais simplement de montrer effectivement comment moi j'agis, en me disant peut-être que ça peut inspirer les gens. Je pense que c'est à chacun de réaliser, à force de scandales. En fait, c'est important aussi d'attirer l'attention des gens sur différents scandales qui peuvent sortir et pour leur dire « Voilà ce que peuvent être les impacts plus tard » (#5)

¹⁰⁸ MSF : Médecins Sans Frontières et RSF : Reporters Sans Frontières

1.3. Actions institutionnelles

Nous avons précédemment identifié quatre actions institutionnelles (cf. Figure 27) : (i) la plainte à l'entreprise, (ii) la plainte à un tiers (e.g., associations de défense), (iii) la plainte au régulateur (e.g., CNIL en France), (iv) l'action légale. Par rapport à cette catégorisation :

- Nous renommons « plainte à l'entreprise » en « signalement à l'entreprise » ;
- Nous supprimons la catégorie « plainte à un tiers », ayant constaté que cela ne se produisait jamais (tout en soulignant qu'un apport de cette recherche pourrait être de favoriser la possibilité de recourir à l'aide d'organisations tierces) ;
- Nous gardons « plainte au régulateur » (explicitement nommé CNIL) ;
- Nous renommons « action légale » en « recours en justice ».

Nous précisons chacune de ces actions ci-après.

1.3.1. *Signalement à l'entreprise*

Les plaintes à des associations de consommateur (ou des tiers en général) n'ont jamais été citées, en cohérence avec les difficultés que nous avons eues pour les interroger. Il semble donc qu'il existe une marge d'amélioration sur ce point. En outre, la plainte à un tiers relève plus d'une dynamique collective et devrait être classée dans les actions sociales. Nous supprimons cette catégorie comme action institutionnelle.

La plainte à l'entreprise est plus vécue comme un signalement et une recherche d'informations que comme une plainte. Elle revêt un statut officiel et procédural moindre que les autres types d'actions. Pour cette raison, nous la renommons : « **Signalement à l'entreprise** ». Il s'agit d'une pratique d'un profil de répondants qui disposent d'une procédure et de courriers mis en place et qui sollicitent les entreprises à chaque fois qu'un courrier ou un mail est reçu sans justification. Il ne semble pas qu'il s'agisse d'un profil contestataire particulier, mais plus un **fort attachement au respect du droit et du RGPD**. L'objectif est de bien faire appliquer les droits apportés par le RGPD : consentement, retrait et effacement, qui ne sont pas des actions techniques (comme précédemment indiqué dans la Figure 27, mais des actions institutionnelles). Une fois mise en place, cette procédure est assez **simple**, et ne demande que de la motivation et de l'opiniâtreté : « *à chaque fois que je reçois un courrier (...) ou un mail (...), d'une société dans laquelle j'ai jamais mis les pieds, c'est de leur demander comment ils ont eu mes données, pourquoi ils me contactent* » (#15), « *une autre de mes petites routines (...)* »

quand je reçois des appels ou des mails non sollicités, j'ai (un ...) courrier que j'envoie régulièrement dès que je reçois ce type de sollicitations » (#9), « Ça ne prend pas beaucoup de temps en soi » (#15).

De plus, le signalement à l'entreprise semble surtout relever d'un échange cordial avec une entreprise pour savoir comment elle s'est procuré les données et rétablir la situation. Cet échange est d'autant plus cordial s'il s'agit d'une PME : il y a une tolérance pour les plus petits (qui peuvent manquer de moyens ou de connaissances). Il s'agit d'un comportement entre l'hygiène numérique et une action menée pour le bienfait de la société (les expressions « *effet Colibri* » et « *effet Chevalier Blanc* » sont citées).

Une procédure peut également être ajoutée dans cette catégorie de signalement : les déclarations aux opérateurs Telecom (e.g., service Abuse d'Orange¹⁰⁹). De même, cette action est simple, demande peu de temps, semble généralement efficace et répond à un objectif de rétablir une situation défaillante.

1.3.2. Plainte à la CNIL

La plainte à la CNIL a fait l'objet de très nombreux échanges avec les répondants, ces derniers ne sont pas opposés à la CNIL et en soulignent les bénéfices en termes de sensibilisation de la population et de contre-pouvoir. Deux répondants ont déjà postulé à des offres d'emploi à la CNIL. Mais, plusieurs obstacles entravent le recours à la plainte auprès de la CNIL (cf. Tableau 42). Premièrement, nos résultats suggèrent que des compétences techniques et juridiques sont nécessaires pour porter une plainte (efficace) auprès de la CNIL (1). Deuxièmement, les répondants soulignent le manque de moyens de la CNIL (2) mais également le manque de légitimité en comparaison avec un recours en justice (3). Ceci est d'autant plus vérifié dans le cas de violations de données personnelles graves : la CNIL ne sera pas saisie, mais des actions en justice vont être conduites (contrairement aux moyens recommandés par les autorités après une violation de données). Et ceci est cohérent avec les principaux motifs de plainte enregistrés par la CNIL, i.e., la surveillance au travail et la prospection commerciale (cf. Annexe 10) : les violations de données personnelles ne font pas partie des motifs principaux de plaintes déposées

¹⁰⁹ https://assistance.orange.fr/ordinateurs-peripheriques/depanner/probleme-de-mail/probleme-avec-la-reception-de-mails-douteux/le-service-abuse-presentation_206348-41412

à la CNIL. Enfin, certains s'interrogent sur le manque d'objectivité de la CNIL et une possible orientation politique et gouvernementale dans ses actions (4). Nous reprenons cela dans le Tableau 42.

Tableau 42 : Avantages et inconvénients des actions conduites auprès de la CNIL

Attributs concernant la CNIL	Verbatims illustratifs
1. Procédure qui nécessite des compétences juridiques et techniques pour être efficace	« Je pense qu'on n'a pas (...) la capacité de saisir ces enjeux juridiques là (...) Pour moi, la CNIL (est ...) sur des formulations très juridiques » (#1) « (la) personne qui va prendre le temps pour aller porter plainte à la CNIL (...) est une personne qui a confiance dans le processus, qui sait par quel bout attraper le machin, par où commencer, tirer le fil à trouver pour tirer après la pelote. C'est une personne qui a du temps. C'est une personne qui a de bonnes connaissances juridiques dans le domaine sans être un avocat spécialiste de la privacy. C'est une personne qui est opiniâtre. » (#12) « c'est assez pratique et efficace (mais ...)il faut être friendly avec le numérique un petit peu » (#2)
2. Manque de moyens	« Elle est absolument sous-équipée, aussi en termes d'effectifs pour effectuer une forme, voilà, de contrôle sur les domaines qu'elle est sensée contrôler » (#1) « C'est que de toute façon, ils n'auront pas les moyens de traiter ma plainte. Autant qu'ils s'attaquent à de gros morceaux » (#12)
3. Manque de légitimité et d'efficacité par rapport à une action juridique classique	« je ne vois pas l'intérêt d'aller voir la CNIL pour dire « Je me suis fait pirater » si je me suis fait pirater effectivement, mon 1er réflexe, ça serait d'aller voir un informaticien pour qu'il voie si je suis infecté, qu'est-ce qui est infecté, qu'il récupère le maximum de données » (#14) « je porte plainte (mais ...) je porte plainte pénalement (et ensuite ...) via les structures type CNIL » (#2) « Je suis allé au tribunal administratif pour une réponse de la CNIL (... qui) était très lacunaire et simple (...) J'ai juste eu (...) une réponse par mail en disant qu'ils avaient fait le nécessaire (...) Ils ne citaient aucune source de droit, donc pour moi, j'aurais bien aimé avoir des sources de droit » (#4) « (Si piratage de la CNAM) Je porte plainte à l'État » (#14) « Et en fait, ceux qui ont porté plainte, ce sont par exemple la Quadra sur, ben, l'usage des drones, mais ils n'ont pas porté plainte auprès de la CNIL. Euh, enfin, ils sont passés par le Conseil d'État. Enfin, ça a été, ce sont des parcours, voilà, juridiques plus larges. Ben du coup, voilà, est-ce que j'aurais pu porter plainte sur des questions de ce genre ? » (#1)
4. Manque d'objectivité (objet d'une certaine orientation politique)	« je me demande si elle (la CNIL) ne sert pas de caution – (...) pour montrer qu'on agit du côté de la vie privée au niveau du gouvernement, mais que dans les faits, on ne lui donne pas les moyens de ses missions. » (#5) « peut-être des orientations politiques qui, à mon avis, sont données et qui fait que ça ne bouge pas. Manque de moyens évident, quoique la CNIL espagnole a à peu près les mêmes moyens et condamne quasiment 100 fois plus que la CNIL » (#8)

1.3.3. Recours en justice

Plusieurs **actions en justice** ont été citées : (i) plainte au Conseil d'État, (ii) plainte à un tribunal, (iii) saisine en référé. Elles sont rares et le fruit d'actions collectives et militantes, ou d'individus a priori isolés, mais soutenus dans des groupes d'échange.

Enfin, l'analyse des réactions dans le cas de violations de données personnelles ne fait pas apparaître de nouveaux types d'actions. Nous observons essentiellement un renforcement des actions habituellement conduites, mais également une très grande résignation amenant la majorité des répondants à ne pas agir. Nous les précisons page suivante.

1.4. Réponses face à une violation de données personnelles

Face à une violation de données personnelles telles que celles de la Caisse Nationale d'Assurance Maladie, les répondants vont **reproduire des comportements habituels** :

- Une personne ayant pour habitude de faire du « name and shame » va poster des messages sur les réseaux sociaux : *« Je vais surtout poster, publier l'info (...) Pour qu'elle soit connue par le plus grand nombre (...) Pour les sensibiliser et puis pour « name showing » (#3)*
- Le « name and shame » peut s'accompagner d'une recherche technique préalable (toujours reproduction d'un comportement habituel du répondant) : *« Alors, je me renseigne. (...) si les données sont publiques, je les télécharge. (...) si j'ai moyen de remonter les gens qui ont fait ça, ce qui est très peu probable, parce que je n'aurai pas accès aux infos. S'il y a moyen, je les remonte, juste pour le plaisir. Si j'ai moyen... Si j'apprends que c'est vraiment parce qu'ils ont fait une énorme erreur entre guillemets impardonnable du côté de la Caisse d'Assurance Maladie, ben, je vais faire en sorte qu'ils soient sanctionnés pour ça, parce que voilà, je trouve ça important (...) Donc je vais me faire plaisir, pour bien montrer que la prochaine fois, il va falloir faire un effort » (#7)*
- Et une personne ayant pour habitude de porter plainte va également le faire : *« Je porte plainte pénalement, mais aussi via les structures type CNIL (...) pour le notifier et que ça soit écrit quelque part que j'ai bien conscience et que j'ai porté plainte parce que du coup, voilà, juridiquement, ça va pouvoir me servir après, si j'ai besoin de faire une action » (#2) ; « Je porte plainte à l'État » (#14)*

De plus, et comme précédemment souligné, dans le cas d'une violation de données personnelles, **la CNIL ne sera pas saisie en premier lieu**, mais des actions en justice vont être conduites.

Il est à noter que beaucoup de personnes interrogées **ne vont pas agir**, car elles se sentent totalement démunies. En effet, dans le cas des violations de données personnelles, les compétences et croyances, telles que la résignation ou la nécessité du collectif (protection et force du groupe) sont encore plus prégnantes : nous les verrons dans le paragraphe 3.4.

2. Conséquences et valeurs culturelles identifiées

Le codage des données a permis d'aboutir à la définition de : 10 types d'actions, 16 conséquences, et 5 valeurs (détaillés dans le Tableau 43 ci-dessous ; cf. Tableau 44 et Tableau 45 pour les verbatims illustratifs).

Tableau 43 : Éléments du chaînage cognitif

Types d'actions	1. Signalement 2. Plaintes CNIL 3. Recours en justice 4. Formation support 5. Sensibilisation 6. Name and shame 7. Militantisme 8. Brouillage digital 9. Hygiène digitale 10. Protection technique
Conséquences	11. Limiter le SPAM 12. Limiter le scoring 13. Garder le contrôle de ses données personnelles 14. Garder son jardin secret 15. Faire appliquer le droit 16. Sensibiliser au risque 17. Former à la technologie 18. Développer des actions de groupe 19. Protéger un bien commun 20. Rendre la technologie positive 21. Sécuriser 22. Permettre l'anonymat 23. Limiter le privacy washing 24. Freiner l'économie des données 25. Limiter la surveillance étatique 26. Militer pour des idéologies
Valeurs	27. Liberté 28. Sécurité 29. Transparence 30. Individualité 31. Équité sociale

Tableau 44 : Verbatims illustratifs des conséquences

Conséquences	Verbatims illustratifs
11. Limiter le SPAM	« les sollicitations pour de la publicité (...) la volonté de la publicité est de me faire faire des choix, de me guider ou de me pousser à faire des choix qui ne seraient pas forcément les miens » (#9)
12. Limiter le scoring	« je n'aimerais pas que (...) toutes mes fiches de santé se retrouvent entre les mains de ma banque (...). Ils pourraient me facturer plus (...) Ma banque, pour l'accord d'un prêt pourrait me dire « Oui, mais là, au vu de vos frais de santé, on va vous faire payer plus cher l'assurance du crédit parce qu'on n'est pas surs que dans 30 ans, vous soyez encore en vie ». (#14)
13. Garder le contrôle de ses données	« je suis assez sensible à ça, voilà, je n'aime pas que tout ça se balade sans savoir ce qui se balade sur moi un peu partout, quoi » (#15)
14. Garder son jardin secret	« l'expression « je n'ai rien à cacher donc je peux le montrer », ça ne m'intéresse pas (...). J'ai le droit d'avoir mon espace même si dans ma vie, il n'y a rien d'exceptionnel (...) mais je me dis « Ça reste intime, ça reste mon histoire et je raconte à l'extérieur que ce que moi je choisis de raconter. » (#6)
15. Faire appliquer le droit	« J'aime bien le RGPD, j'aimerais bien qu'il soit appliqué, écouté, respecté (...) Je dis toujours cette phrase « Les droits ne s'usent que si on ne s'en sert pas » et j'aime bien l'utiliser à propos du RGPD » (#9)
19. Protéger un bien commun	« c'est faire en sorte que mon action, elle améliore le bien-être des gens, des humains, ou même des animaux, (...) quand on rentre dans la technologie (...) elle doit être là pour faire en sorte qu'à la fin, les gens soient heureux. Et les gens sont heureux s'ils sont libres. Et pour qu'ils soient libres, il faut qu'ils aient une certaine autonomie d'action, qu'ils n'aient pas une épée de Damoclès, que ce soit un contrôle social par le haut par l'État ; par le bas (...) où le groupe a toujours une espèce de regard constant sur l'individu » (#7)
20. Rendre la technologie positive	« je suis pour l'open data. (...) Moi, j'adore regarder les stats de l'Insee (...). Parce que je sais que c'est traité de façon respectueuse de la réglementation et donc de la vie privée. Que l'Insee en France ne descende pas à moins d'un kilomètre pour justement éviter qu'on puisse identifier des gens » (#12) « Shrems, ce qu'il fait, c'est génial : il rend effectif le RGPD grâce à des actions de groupe » (#5)
21. Sécuriser	« actuellement, vu que je suis chef d'entreprise, je me dis « Faut que je sécurise » (...) la sécurité, c'est toujours un ratio entre l'accessibilité, la facilité d'utilisation et la sécurité opérationnelle » (#14)
22. Permettre l'anonymat	« Tu vois, c'est comme le chiffrement. Plus on est de gens à utiliser du chiffrement de mails, moins ceux qui en ont véritablement besoin vont être visibles » (#13)
26. Militer pour des idéologies	« les gens qui cherchent à se mobiliser pour les questions de protection des données personnelles (sont ...) des gens dont la motivation première, elle est idéologique (...) des anarchistes, des gens comme ça qui vont avoir une vision du monde et dans leur vision du monde, la surveillance et ce genre de choses et même la technique sont négatives » (#7)

Tableau 45 : Verbatims illustratifs des valeurs

Conséquences	Valeurs
1. Liberté	« Je pense qu'il y a un aspect qui me nourrit depuis très longtemps (...) c'est le respect de la liberté (..), je parlais d'atteinte à ma liberté, à mon libre arbitre (...) s'il y a une valeur qui est primordiale, c'est ça » (#9) « La liberté, pour moi, c'est le choix » (#12) « Une liberté de choix et les moyens d'atteindre cette liberté de choix, c'est à travers distribuer des compétences de savoir identifier un site fiable, savoir rajouter un bloqueur de publicités, savoir bloquer, savoir rajouter un bloqueur de tracker » (#6)
2. Sécurité	« On fait des choses qui ne sont pas malveillantes, on a besoin que notre anonymat soit respecté, que notre vie privée soit respectée (...) je me demande parfois si le fait que mes prises de position, ils ne sont pas d'accord avec et qu'ils pensent que je ne vais pas respecter le droit de réserve » (#4)
3. Transparence	« En fait c'est qu'on n'apprend pas aux gens ce qui se passe derrière un logiciel. Qu'après, les gens ils le fassent en connaissance de cause, c'est une chose » (#13) « Valeur de transparence, de comment le système il est construit » (#2) « Pour que ça cesse, quoi et d'arrêter de prendre les gens pour des cons, quoi » (#8) « Quand on a un problème lié à de la donnée personnelle et qu'on n'est pas malveillant à la base, le mieux, c'est d'être le plus transparent possible vis-à-vis des utilisateurs » (#7)
4. Individualité	« Eh ben parce que je n'ai pas envie que n'importe qui vienne mettre le nez dans mes affaires. C'est très égoïste (...) même si je n'ai rien à me reprocher, même si soi-disant, je n'ai rien à cacher. On a toujours quelque chose à cacher » (#12)
5. Équité sociale	« Je les maîtrise, je fais en sorte pour que vous puissiez les maîtriser aussi et vous amener à mon niveau » (#6) « Il faut qu'il y ait de la diversité. Internet, c'est ça, c'est qu'on puisse trouver plein de choses qui puissent convenir à tout le monde » (#13) « Des personnes qui sont en situation de handicap que des personnes qui subissent des violences physiques que des femmes qui sont en situation de risque, que des enfants (...)...C'est vital pour elles d'être invisibles sur Internet (...) elles ont besoin de communiquer, ça peut être avec des journalistes (...) c'est pour elles que je chiffre aussi des messages » (#13) « Et je pense aux gens qui ont des addictions, par exemple. Les addictions aux jeux, à l'alcool, mais aussi à des addictions complètement...l'achat compulsif. Ça paraît bête. Vous pouvez vite cibler des gens parfois jeunes là-dessus. Et ça, ça me révolte énormément. Et ça, ça me fait peur » (#3) « C'est ça qui me ferait vraiment monter sur les barricades. C'est profiter de la vulnérabilité des gens » (#3)

Section 5. Résultats analytiques de la recherche

Conformément à l'approche montrée dans la Figure 32, la section 5 est consacrée aux résultats analytiques (dans la section 5), autour de deux parties : les motivations socio-culturelles dominantes (1) et les pratiques sociales de protection de la vie privée (2).

1. Motivations socio-culturelles dominantes

Comme nous l'avons expliqué page 243, sur la base du nombre de citations et de la force des associations, les trois motivations culturelles dominantes sont : Équité sociale (3.1.), liberté (3.2.), et sécurité (3.2.). Nous décrivons ces motivations culturelles dans les pages suivantes.

1.1. Équité sociale : première motivation culturelle

Nos résultats suggèrent que la défense d'une équité sociale, basée sur des principes d'égalité, d'intérêt collectif et de défense des plus vulnérables, est une motivation culturelle essentielle dans la mise en place d'actions de protection des données personnelles. Dans l'objectif de défendre une diversité et une égalité sociales, elle permet à l'aide de moyens techniques aux plus vulnérables de garder des informations confidentielles, à l'aide d'actions sociales de développer une conscience des risques et des enjeux de la protection de la vie privée et à l'aide de moyens institutionnels de faire vivre et appliquer le droit.

Par conséquent, l'équité, i.e., « la qualité consistant à attribuer à chacun ce qui lui est dû par référence aux principes de la justice naturelle »¹¹⁰, consiste à ajuster des actions et des décisions selon des critères d'inégalité et en fonction de ce qui est jugé juste et équilibré entre les individus. L'équité est un concept éthique qui fait référence aux questions de justice entre individus (Kolm, 2002), et notamment de répartition des richesses entre individus, pouvant nécessiter l'intervention possible de l'État (justice sociale). L'équité est un principe de justice distributive, i.e., principe selon lequel les individus sont par nature inégaux entre eux donc doivent être traités inégalement, alors que l'égalité est un principe de justice commutative, i.e. principe selon lequel les individus égaux entre eux, indépendamment de leur origine ethnique

¹¹⁰ <https://www.larousse.fr/dictionnaires/francais/équité/>

ou de leur genre par exemple, et doivent être traités également (Aristote, s. d.)¹¹¹. Cela se traduit dans les systèmes de contributions sociales : selon un principe d'équité, les individus qui ne sont pas égaux en termes de revenus doivent contribuer de manière inégale à un régime fiscal ; ou selon un principe d'égalité, certaines allocations sociales sont attribuées de façon strictement égalitaire indépendamment du revenu des personnes et non soumises à condition de revenus.

L'équité sociale telle que définie dans notre recherche recouvre les notions d'équité (terme « équité » cité majoritairement par les répondants), et inclut également les notions de « diversité sociale », de « défense des plus faibles » et « d'intérêt collectif ». Ainsi, le concept d'équité sociale recouvre les valeurs culturelles :

- d'interdépendance (Sharma, 2010), i.e., le fait d'appartenir et d'agir pour un groupe social, avec une importance donnée aux objectifs collectifs plus qu'individuels ;
- d'égalité sociale (Sharma, 2010), i.e., le degré selon lequel les inégalités entre personnes d'une même société ne sont pas acceptées comme normales,
- de distance hiérarchique (Hofstede, 1984), i.e., le degré selon lequel les membres les moins puissants d'une société acceptent et s'attendent à ce que le pouvoir soit distribué de manière inégale,
- d'égalité des genres (Hofstede, 1984; Sharma, 2010),
- et d'égalitarisme (Schwartz, 1994), i.e., la volonté d'une égalité des chances égales entre tous, et d'universalisme (Schwartz, 2006), i.e., le souci des faibles, de ceux qui sont les plus susceptibles de souffrir des politiques économiques centrées sur le marché.

Nous définissons l'équité sociale comme le souhait que chaque individu ait les mêmes droits et les mêmes possibilités, indépendamment des différences sociales, de genre, d'origine, de religion et de vulnérabilité, dans l'objectif collectif de protéger un bien commun.

Les individus vont agir pour la protection des données personnelles, dans un objectif d'équité sociale pour deux raisons : (i) pour défendre ceux qui n'en n'ont pas les moyens ou les capacités techniques, faisant le constat d'un déséquilibre tant dans les capacités techniques en général (e.g., fracture numérique) que dans les possibilités de protection et de défense de ses

¹¹¹ Ethique à Nicomaque (V,15) : « L'équitable tout en étant le juste n'est pas le juste selon la loi, mais un correctif de la justice légale. La raison en est que la loi est toujours quelque chose en général, et qu'il y a des cas d'espèce pour lesquels il n'est pas possible de poser un énoncé général qui s'y applique avec rectitude ».

données personnelles, (ii) pour défendre ceux qui sont dans la nécessité de rester anonymes (partant du principe que certains ont peut-être plus besoin de garder certaines informations confidentielles que d'autres). En somme, l'équité sociale est une motivation essentielle pour la défense des données personnelles, car tout le monde n'est pas égal « devant la technique ».

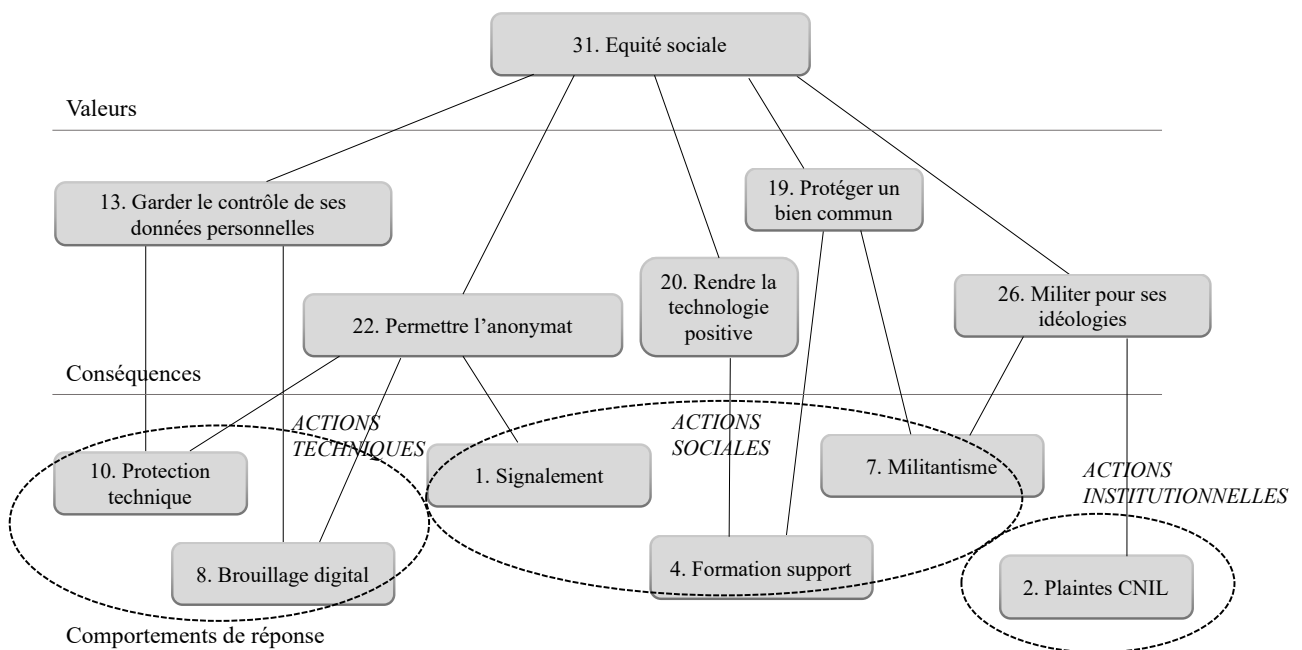
De plus, l'équité est un fondement de la culture « tech » et « hacker » dont est issue une majorité des professionnels en systèmes d'information et de personnes investies pour la défense de la vie privée numérique, défenseurs d'un Internet libre, ouvert et démocratisé. Par exemple, John Perry Barlow écrit en 1996 dans la Déclaration d'indépendance du cyberspace : « *Nous créons un monde où tous peuvent entrer, sans privilège ni préjugé dicté par la race, le pouvoir économique, la puissance militaire ou le lieu de naissance* »¹¹².

Enfin, cet objectif d'équité peut être atteint par trois moyens :

- par le contrôle de ses données personnelles, i.e., une des principales dimensions de la préoccupation pour la protection de la vie privée (Belanger et al., 2002; Malhotra et al., 2004; Smith et al., 2011). Le contrôle de ses données personnelles passe par des actions techniques (brouillage digital, protection technique). De plus, l'utilisation de ces actions techniques répond à un souhait de rendre ces moyens techniques actifs et utilisables par tous, toujours dans un objectif de défense d'un bien commun et d'une équité sociale ;
- par des actions sociales, selon 3 logiques : (i) en rappelant le respect de la loi à certaines entreprises (« signalement ») lorsqu'un mauvais usage des données personnelles est identifié et pour permettre un respect de l'anonymat de tous ; (ii) en apportant un support et des formations pour développer un usage éclairé et positif de la technologie ; (iii) par des actions militantes dans un objectif de défense de l'intérêt général ;
- par l'application du droit, essentiellement à travers le dépôt de plaintes à la CNIL. Cette application du droit a pour objectif de « faire vivre » le droit, de ne pas le laisser comme lettre morte, voire de le renforcer. De plus, le recours au droit a pour objectif de défendre des cas individuels constatés, mais également des cas plus collectifs. Ce recours au droit peut avoir pour finalité de militer pour des idéologies.

¹¹² Déclaration du cyberspace, disponible le 12.11.2022 à :
https://fr.wikipedia.org/wiki/D%C3%A9claration_d%27ind%C3%A9pendance_du_cyberspace

Figure 34 : Schéma motivationnel pour des valeurs d'équité¹¹³



En somme, le premier schéma motivationnel (cf. Figure 34) dominant montre que les individus agissent dans une volonté d'équité sociale (reposant sur des principes d'égalité, d'intérêt collectif, de défense des plus vulnérables) face à des inégalités de compétences techniques (en particulier en matière de protection de la vie privée) et des inégalités de besoins de confidentialité (les personnes les plus vulnérables ayant souvent besoin de plus cacher leur vulnérabilité). Pour cela, ces personnes vont agir en recourant à l'application du droit (plaintes CNIL) pour eux-mêmes ou de façon plus collective, et par des actions techniques, pour eux-mêmes et en rendant ces moyens de protection efficaces donc disponibles pour tous, et par des actions sociales et militantes (pour un développement éclairé de la technique).

¹¹³ Ne figurent sur ce schéma motivationnel que les conséquences citées au minimum 3 fois et les comportements de réponse cités au minimum 2 fois

1.2. Liberté : deuxième motivation culturelle

La liberté (de choix ou d'action) est la deuxième motivation culturelle la plus importante. La liberté étant « l'état de quelqu'un qui n'est pas soumis à un maître »¹¹⁴, ceci est tout à fait cohérent avec de précédentes recherches indiquant que plus les personnes acceptent les différences de pouvoir entre les membres d'un même groupe (dimension de distance hiérarchique ; Hofstede, 1984), plus elles peuvent accepter de livrer une partie de leur vie privée à un autre, supérieur hiérarchiquement et plus autoritaire. Ceci signifie que plus les individus acceptent un pouvoir hiérarchique (et plus ils acceptent une liberté restreinte), moins leur préoccupation pour la protection de leurs données personnelles est importante. De plus, les cultures valorisant une forte distance hiérarchique connaissent une norme de contrôle et d'autorité plus formelle, qui s'accompagne d'un partage de l'information centralisé et restreint (Lowry et al., 2011). Il est admis que des informations personnelles soient connues (i.e., partager son état de santé et ses feuilles de sécurité sociale avec son employeur) et qu'un contrôle social (avec utilisation des technologies) soit exercé. Ceci est conforme aux travaux de Bellman et al. (2004) ainsi que Cao & Everard (2008) qui ont trouvé une relation négative entre la dimension de distance hiérarchique (Hofstede, 1980) et la préoccupation pour la protection des données personnelles.

Deuxièmement, l'importance de la notion de liberté comme valeur motivationnelle pour la protection des données personnelles est également logique, car la protection de la vie privée a été institutionnalisée dans un objectif de protection des libertés fondamentales dans le cadre de la Déclaration universelle des droits de l'homme en 1948 : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » (Article 12). La vie privée est liée à la notion de liberté dans des sociétés démocratiques (Vallet, 2012) : toutes les personnes interrogées sont sensibles et attachées au lien entre protection de la vie privée et liberté.

Troisièmement, le fait que la liberté soit la deuxième valeur motivationnelle citée n'est également pas étonnant car liberté et équité sont liées. Selon la théorie de la justice (Rawls, 1971), liberté et équité peuvent être associées car les inégalités sont tolérables à condition que tous bénéficient d'une égalité des chances pour accéder à des positions plus favorables. Il s'agit

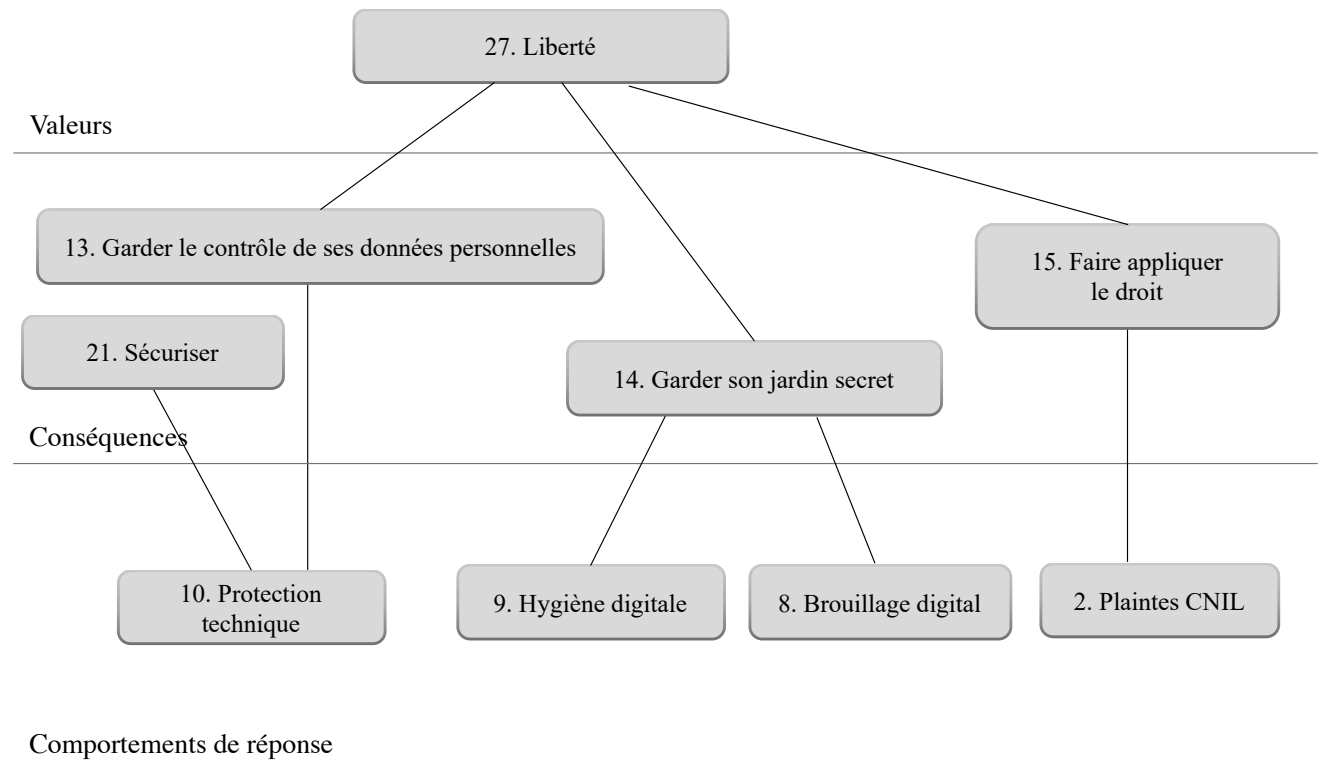
¹¹⁴ <https://www.larousse.fr/dictionnaires/francais/liberte>

du principe de discrimination positive. Pour exemple, un répondant nous indique : « *Ma liberté à moi m'intéresse assez peu si elle n'est pas partagée par tout le monde* » (#9).

Cet objectif de liberté peut être atteint par deux moyens (cf. Figure 35) :

- par des actions techniques, ayant pour objectif de sécuriser l'accès à leurs données et de garder le contrôle de leurs données personnelles (action de « protection technique ») et de façon plus simple de « garder son jardin secret » (actions d'hygiène ou de brouillage digitaux) ;
- par des plaintes à la CNIL dans l'objectif de faire appliquer le droit.

Figure 35 : Schéma motivationnel pour des valeurs de liberté¹¹⁵



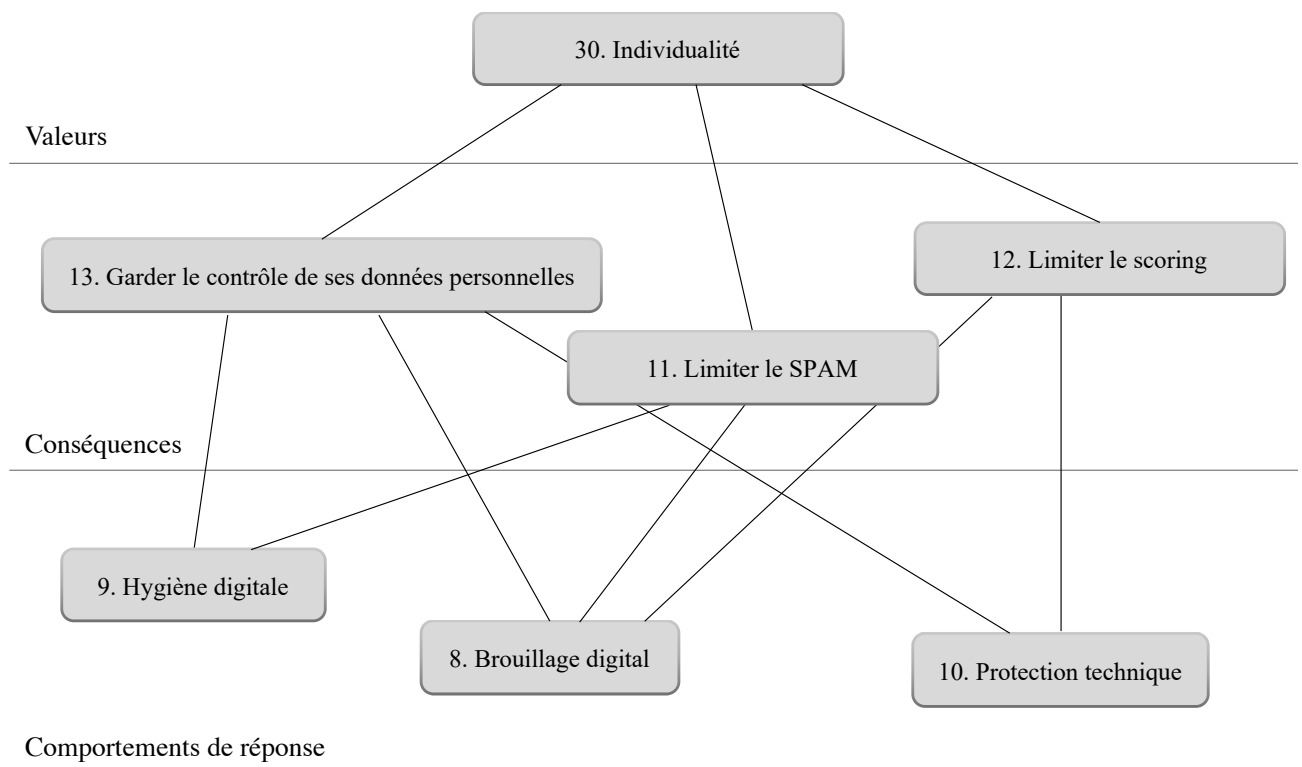
¹¹⁵ Ne figurent sur ce schéma motivationnel que les conséquences citées au minimum 2 fois

1.3. Sécurité : troisième motivation culturelle

La troisième motivation culturelle est l'individualité, i.e., la protection de son identité numérique et de sa tranquillité individuelles, parfois de façon « *très égoïste* » (#12). L'individualité correspond à la protection de sa tranquillité, de son autonomie (*affective autonomy, intellectual autonomy* ; Schwartz, 2006) et de son intimité. Autonomie et intimité sont liées : l'autonomie est la capacité à protéger sa propre intimité (par exemple, la perte d'autonomie chez les personnes âgées correspond à la perte d'intimité du corps).

Pour cela, les personnes se concentrent sur les actions techniques pour garder le contrôle de leurs données personnelles. Les actions techniques ne répondent pas à une cause sociale collective particulière mais reflètent plutôt le désir de rester caché (pour des raisons qui peuvent être très diverses). Ces actions techniques ont également pour objectif de protéger sa tranquillité de deux manières : (i) en limitant le *scoring*, i.e., l'accès limité à certains services ou la surfacturation de certains services, sur la base de l'exploitation de données personnelles collectées par ailleurs (e.g., surfacturation de frais de couverture médicale selon des données médicales obtenues) ; (ii) en limitant le SPAM, i.e., la prospection commerciale, afin de garder sa tranquillité et son espace personnel sans perception d'intrusion (cf. Figure 36 page suivante).

Nous retrouvons une continuité avec les résultats précédents car liberté et individualité sont liées. Ainsi, un répondant nous indique également : « *Les gens sont heureux s'ils sont libres. Et pour qu'ils soient libres, (...) il faut qu'ils aient une certaine autonomie d'action, qu'ils n'aient pas une épée de Damoclès, que ce soit un contrôle social par le haut par l'État ; par le bas une espèce de chappe de plomb, de qu'en dira-t-on où on est épié, où le groupe a toujours une espèce de regard constant sur l'individu* » (#7).

Figure 36 : Schéma motivationnel pour des valeurs d'individualité¹¹⁶

Nous soutenons que ce souhait de contrôle de son autonomie, intimité et tranquillité vise un objectif de **sécurité individuelle, de sécurité familiale et d’imaginaire de sécurité** (comme préserver la chaleur du foyer, ne pas perturber sa quiétude, se sentir tranquille, cultiver son jardin secret, être protégé). Parmi les valeurs de Schwartz (2006), le droit à la vie privée (i.e., ne pas être exposé aux regards indiscrets) est une valeur proche de la sécurité familiale (i.e., sécurité pour ceux qu’on aime). Enfin, l’autonomie et l’intimité apportent la sécurité. Par exemple, une femme est à la recherche de son autonomie financière pour être indépendante et ainsi se protéger de toute situation de dépendance présentant des risques pour elle. L’intimité permet à chacun, enfant ou parent, de vivre des moments agréables et chaleureux, de se sentir protégé face aux risques de la vie extérieure.

C’est pourquoi nous concluons sur une troisième motivation culturelle qui repose essentiellement sur un souhait de sécurité individuelle : la protection de son individualité, de son intimité et de son autonomie apporte une sécurité personnelle, réelle ou perçue (constitutive d’un imaginaire de sécurité).

¹¹⁶ Ne figurent sur ce schéma motivationnel que les conséquences citées au minimum 2 fois

2. Pratiques sociales de protection de la vie privée

Notre recherche montre d'une part que la défense d'une équité sociale est une motivation essentielle à un engagement pour le respect de la vie privée, et d'autre part que la protection de la vie privée est une pratique sociale. Dans cette dernière partie, nous étudierons comment les dynamiques structurelles des pratiques se construisent (4.1.), mobilisant les schémas motivationnels décrits précédemment. Pour compléter la compréhension des systèmes structurels, nous préciserons ensuite les formes de compétences individuelles (4.2.) et collectives (4.3.) mobilisées.

2.1. Dynamiques structurelles des pratiques de protection de la vie privée

Au fil des entretiens et alors que notre objectif initial était essentiellement d'identifier les valeurs partagées au sein de groupes sociaux pour la protection des données personnelles, les actions de protection de la vie privée apparaissent comme des pratiques sociales, avec différentes caractéristiques (échange social, structure temporelle, activité routinière) :

- La protection de la vie privée n'est pas une activité isolée et est une pratique qui prend naissance et se développe dans un échange social (e.g., « *Enfin, la question, elle ne peut pas être individuelle parce que je trouve que ça met une contrainte telle sur l'individu que du point de vue du vécu, vraiment, genre, c'était horriblement fatigant* » (#1)) ;
- La protection de la vie privée est une pratique qui se construit dans le temps (e.g., « *c'est des choses qui sont construites de manière – comment dire ? – progressive. C'est difficile de... J'ai pas eu un jour un déclic* » (#7)) ;
- Une fois acquises, les actions de protection de la vie privée sont souvent décrites comme des réflexes et activités routinières (« *Je suis habituée à faire certains gestes, certaines opérations. Ça ne me demande plus d'effort, (...) C'est devenu quelque chose de naturel* » (#12)).

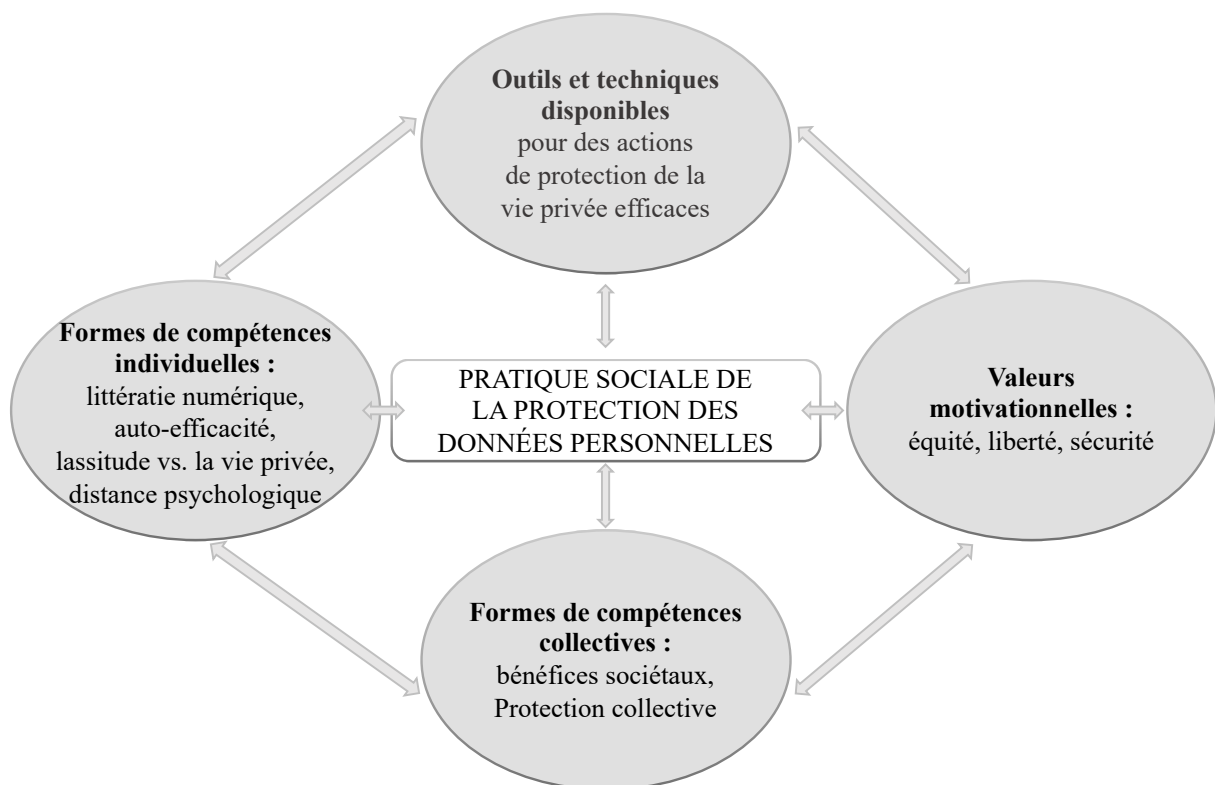
Nos résultats indiquent qu'il n'est pas possible de considérer les actions de protection de données personnelles, surtout dans le cas d'une violation avérée, comme une action individuelle menée par un agent qui va décider seul et rationnellement des actions à mener par la suite. Les actions de protection des données personnelles s'apparentent nettement plus à une pratique, i.e., « *des blocs d'activités, de significations, de compétences et d'objets, (... qui) se transforment*

et se diffusent en « recrutant des individus » qui ensuite les mettent en œuvre de façon routinière » (Dubuisson-Quellier & Plessz, 2013, p.1).

Surtout, les pratiques sociales de protection de la vie privée se développent au sein de structures mobilisant des matériaux (outils et techniques de protection de la vie privée), des compétences et des croyances individuelles et collectives, et des valeurs : « c'est un sujet qu'on pourrait qualifier de différentes manières, mais ce n'est pas un sujet purement technique. Mais pour moi, ce qui va être intéressant, c'est comment est-ce que dans les groupes – parce ça, c'est aussi des dynamiques de groupe, ce n'est pas que des individus tout seuls – la part du technique et la part d'idéologie » (#7).

Dans notre contexte, les matériaux sont les outils et techniques pour mener les actions de protection des données personnelles (techniques, sociales, institutionnelles), les formes de compétences sont individuelles et collectives (que nous précisons dans les paragraphes 4.2 et 4.3 suivants) et les idéaux sont les schémas motivationnels identifiés (équité sociale, liberté, sécurité). Ces trois ensembles de construits interagissent comme précisé dans la Figure 37 page suivante.

Figure 37 : Structure de pratique sociale de protection de la vie privée



Au sein de ces dynamiques, les valeurs culturelles sont un moteur motivationnel puissant pour être engagé pour la protection de ses données personnelles, pour des motivations éthiques qui peuvent être très variées (idéologies politiques fortes, convictions individuelles - e.g., Jan Krum, créateur de WhatsApp, qui est entré en conflit avec Mark Zuckerberg après son rachat par Meta, officiellement pour des raisons de désaccord sur les questions de protection de la vie privée des utilisateurs). Cependant, elles se heurtent souvent à un manque de moyens techniques (outils ergonomiques et accessibles protecteurs de la vie privée), à des compétences limitées (*privacy literacy*), à un sentiment d'inefficacité (*self-efficacy*), voire une certaine résignation (*privacy fatigue*). Ce déséquilibre entre valeurs motivationnelles, matériaux disponibles et compétences freinent le développement de pratiques sociales de protection de la vie privée : « *je ne pense pas que ça dépende des valeurs, malheureusement. Ça dépend plutôt de la formation et en l'occurrence, technique...* » (#5).

En revanche, le développement d'un savoir (articulé autour de compétences, d'une culture numérique et d'une réduction de la distance psychologique avec les risques liés à la violation des données personnelles), et d'un pouvoir (grâce aux développements d'outils techniques accessibles mais également de collectifs permettant la formation, l'entraide et le soutien), minimise l'importance des idéaux et des valeurs culturelles. Un développement équilibré entre idéaux, moyens et formes de compétences permet l'adoption d'une réponse active face à une violation de données personnelles. Enfin, cette approche par la théorie de la pratique permet également de « *saisir les conditions de changement dans des pratiques, en insistant sur la structure temporelle des activités sociales, sur la tension entre routine et réflexivité et sur le rôle des infrastructures matérielles* » (Dubuisson-Quellier & Plessz, 2013, p.1). Ces résultats nous permettent également d'identifier des pistes d'application assez claires, que nous discuterons après avoir détaillé les formes de compétences individuelles et collectives.

2.2. Formes de compétences individuelles pour la protection de la vie privée

Les compétences sont toutes les formes de connaissances et de savoir-faire, de compréhensions, et de croyances, utilisées de manière consciente ou inconsciente dans la réalisation d'une action. Les compétences peuvent s'articuler autour de deux axes : le savoir, i.e., savoir-faire, compétences techniques, et le pouvoir, i.e., les moyens psychologiques permettant l'action, l'état psychologique dans lequel l'agent se trouve lors d'une violation de ses données personnelles, les croyances qui freinent ou motivent l'agent dans l'action. Plus précisément, les croyances sont la représentation ajustée de la réalité, construite à travers les pratiques et les processus de socialisation : les croyances sont le fruit de l'*habitus* de Bourdieu (1972), et d'un « pouvoir-savoir » (Foucault, 1975), i.e., de processus et de luttes qui déterminent les conditions, les formes et les domaines possibles de la connaissance.

Nos résultats suggèrent que dans le cadre des actions pour la protection des données personnelles, les formes de compétence peuvent être soit d'ordre individuel, i.e., relevant d'un état psychologique propre à une personne ou de compétences et de croyances nécessaires à l'action d'un individu seul, soit d'ordre collectif, i.e., mobilisant la force d'un groupe. Chacune de ces formes de compétences fait généralement référence à un concept déjà identifié dans la littérature : notre recherche permet avant tout d'éclairer des interrelations nouvelles entre ces concepts à la lumière d'une approche par la théorie de la pratique.

Ainsi, nous relevons **4 formes de compétences individuelles** (illustrées dans le Tableau 46 ci-après) qui évoluent d'une conscience des enjeux liés à la protection de la vie privée (distance psychologique) à une connaissance de ceux-ci (alphabétisation en matière de vie privée) puis d'un « savoir-pouvoir » (Foucault, 1975), i.e., une capacité à mettre en pratique ces comportements, regroupant une conscience de ses capacités (efficacité personnelle) et un état psychologique le permettant (fatigue). Nous les détaillons ci-dessous.

2.2.1. *Distance psychologique avec les risques liés à la violation de la vie privée.*

- La distance psychologique avec les risques liés à la violation de la vie privée (Bandara et al., 2021; Trope & Liberman, 2010), i.e., la capacité à se représenter mentalement un risque lointain et abstrait de violations de données personnelles et à parcourir mentalement des distances temporelle, spatiale, sociale et hypothétique pour cela.

Nous avons vu que la préoccupation pour la protection de la vie privée était un concept de « haut niveau » (Hallam & Zanella, 2017), distant et abstrait (Bandara et al, 2018) : en d'autres termes, il est nécessaire de faire une projection mentale difficile pour se représenter et prendre conscience des risques liés à la violation des données personnelles. De plus, la distance psychologique affaiblit la relation entre préoccupations en matière de vie privée et comportement défensif (Bandara et al. , 2021).

De la même manière, nos résultats invitent à penser que la distance psychologique avec les risques liés à la violation de la vie privée joue un rôle important dans le développement des actions de protection, mais également qu'il existe plusieurs moyens simples pour développer cette prise de conscience. De façon assez naturelle, l'acquisition de compétences informatiques constitue un levier fondamental pour réduire les risques liés à la violation de la vie privée. Beaucoup d'informaticiens qui savent « ce qui se passe sous le capot » sont attachés à la protection de la vie privée en ligne. Également, les formations de l'ANSII ont permis d'éveiller la conscience des risques chez plusieurs répondants. Enfin, plusieurs livres (e.g., *Discours de la servitude volontaire* de la Boétie, *L'enfer numérique* de Guillaume Pitron »), films (e.g., *La Vague* de Dennis Gansel ou *Truman Show* de Peter Weir), séries (e.g., *Black Mirror* de Charlie Brooker) ou documentaires (e.g., *Citizenfour* de Laura Poitras) ont permis à des répondants de se représenter les risques encourus.

2.2.2. *Alphabétisation en matière de vie privée.*

- L’alphabétisation en matière de vie privée, ou *privacy literacy* (Bartsch & Dienlin, 2016; Trepte et al., 2015; Wissinger & State, 2017), i.e., la maîtrise des compétences nécessaires pour être en capacité de mettre en pratique des comportements en ligne protecteurs de la vie privée.

La protection des données personnelles repose en grande partie sur la responsabilité des utilisateurs qui doivent décider par exemple de communiquer ou non leurs données personnelles (Martin & Murphy, 2017) : il est pour cela nécessaire que les utilisateurs soient en capacité de se protéger et de mettre en pratique des comportements de protection de la vie privée.

L’apprentissage en matière de vie privée dépend de compétences techniques et numériques (i.e., d’une culture numérique : « la vie privée et la culture numérique sont souvent combinées et considérées comme équivalentes » ; Wissinger & State, 2017, p.379), et des connaissances juridiques concernant les réglementations pour la protection de la vie privée. Cependant, il ne suffit pas uniquement de savoir quelles compétences activer et quelles tâches techniques réaliser mais également de comprendre quand et comment des risques nécessitent de le faire. C’est pourquoi l’alphabétisation en matière de vie privée fait également appel à des compétences cognitives, i.e., une capacité individuelle à comprendre, reconnaître, évaluer, percevoir, raisonner et ajuster ses actions (Wissinger & State, 2017). En d’autres termes, l’alphabétisation en matière de vie privée combine des connaissances déclaratives (*knowing that*) et procédurales (*knowing how*) (Trepte et al., 2015).

Cette alphabétisation en matière de vie privée se développe à travers l’expérience d’Internet et l’usage des réseaux sociaux, qui impliquent d’ajuster fréquemment ses comportements de dévoilement, de modifier les paramètres de confidentialité de ses applications et par conséquent, favorisent un comportement plus prudent en matière de protection de la vie privée sur les réseaux sociaux (Bartsch & Dienlin, 2016).

Cette notion est citée par tous nos répondants comme une compétence essentielle. Ils déplorent le manque d’éducation numérique au sein de nos sociétés (*knowing how*), et souhaiteraient un renforcement urgent de ces aspects dans les programmes scolaires. Ils cherchent à compenser ce manque d’éducation par différents moyens : en cherchant à se renseigner individuellement (mais avec beaucoup d’efforts, des limites de compréhension et de langue et dans un parcours

semé de doutes) ou en développant des collectifs permettant d'échanger sur de bonnes pratiques et de donner confiance sur les actions à mener. Il s'agit, dans ce cas, de compétences collectives (cf. ci-après).

2.2.3. *Efficacité personnelle en matière de vie privée.*

- L'efficacité personnelle en matière de vie privée, ou *self-efficacy in privacy management* (Bandura, 1977; Chen & Chen, 2015; Mamonov & Benbunan-Fich, 2018), i.e., le degré selon lequel les utilisateurs sont confiants dans leur capacité à gérer leurs paramètres de confidentialité.

Comme nous l'avons précédemment indiqué, la *self-efficacy* fait référence à la croyance d'un individu en sa capacité à exécuter les comportements nécessaires à la réalisation de performances spécifiques (Bandura, 1977) et a été adaptée au contexte de la protection de la vie privée (i.e., *privacy self-efficacy* ; Mamonov & Benbunan-Fich, 2018). La *privacy self-efficacy* est une dimension souvent mentionnée théoriquement comme jouant un rôle dans les réactions face à des menaces sur les données personnelles (Adhikari & Panda, 2018) : elle renforce les comportements de protection (Baker-Eveleth et al., 2021), quelle que soit la connaissance du risque (Bandara et al., 2021).

Nos résultats suggèrent que ce degré de confiance est très variable selon les individus : une personne interrogée déclare être fortement utilisatrice d'outils techniques *pro-privacy*, alors que ses actions se limitent à ne pas mettre d'informations sur ses propres enfants sur les réseaux sociaux, contrairement à une autre personne interrogée qui se déclare faiblement utilisatrice d'outils techniques *pro-privacy*, alors qu'au quotidien cette personne est très précautionneuse et utilise des logiciels tels que Signal.

2.2.4. *Fatigue liée à la protection de vie privée.*

- La fatigue liée à la protection de la vie privée, ou *privacy fatigue* (Choi et al., 2018), i.e., un concept multidimensionnel incluant épuisement et cynisme, sentiment de perte de contrôle lié à la difficulté croissante de gérer ses données personnelles en ligne, et sentiment de futilité dû aux violations répétées des données des consommateurs.

La fatigue liée à la protection de la vie privée joue un rôle essentiel dans les actions qu'un individu va choisir de conduire seul pour la protection de sa vie privée en ligne. Cette fatigue peut aller d'une simple résignation et insatisfaction, souvent liées à la vulnérabilité ressentie, due à la compréhension que les dispositions des entreprises en matière de transparence et de contrôle ne sont pas garanties (Bansal & Zahedi, 2015; Martin, 2018), à un stress général et des émotions négatives causés par la violation de données (Labrecque, 2021). Cette fatigue peut devenir une phobie : une répondante cite l'exemple d'une jeune femme se coupant totalement du monde car étant totalement paniquée par les risques liés aux violations de vie privée. Enfin, la fatigue et la résignation sont encore plus marquées dans le cas d'une violation de données personnelles avérée.

Tableau 46 : Formes de compétences individuelles

Formes de compétences individuelles	Verbatims illustratifs
Distance psychologique liée aux risques de violation	« il suffit d'y mettre un petit peu d'effort au début et je trouve que ça se prend quand même très facilement en main. Donc oui, c'est à la portée de tous dès qu'on est..., dès qu'on comprend l'intérêt » (#5)
Alphabétisation en matière de vie privée	« Parce qu'en fait (...) c'est un manque d'éducation à la base. On reproche beaucoup de choses à l'Éducation nationale (...) il n'y a pas forcément assez d'éducation numérique (...) basique qui pose (...) les bases de (...) la protection de leurs données » (#10) « en fait il faut tout simplement former les citoyens aux outils numériques, pour qu'ils comprennent ce que c'est que hacker, pour qu'ils comprennent ce que c'est un vol de données et là, ils vont vraiment comprendre. Parce que sinon, je pense que les gens, ça leur paraît trop abstrait » (#5)
Efficacité personnelle en matière de vie privée	« Alors, moi, je n'ai pas l'impression de vraiment la protéger au maximum » (#6) « ce n'est pas évident justement de savoir quelles pratiques, quelles bonnes pratiques avoir et de comprendre » (#10)
Fatigue liée à la protection de la vie privée	« Donc on essaie de faire un petit peu comme on peut (...), mais ce n'est jamais facile de tout faire parfaitement (...) Je sais que ça ne sert pas à grand-chose parce que des gens vraiment forts, ben, arriveront à vous traquer » (#10) « Ben c'est bien là le problème, en fait, c'est qu'on est complètement désemparés. Ces données qui ne nous appartiennent plus et sur lesquels on ne détient plus aucun pouvoir. Donc, il ne nous reste que nos yeux pour pleurer. On peut s'indigner si on veut, mais au final, euh, on ne peut rien faire de concret » (#15) « Déjà, je réagis intérieurement en disant « Encore une !, ça n'a rien d'étonnant (...) en tant que citoyenne, je me sens dépassée, voire résignée (...) j'ai vraiment envie d'agir à une échelle plus large en me disant qu'il faut réformer le RGPD, il faut donner plus de pouvoir à la CNIL, il faut faire plus de procès. Mais c'est vrai qu'au niveau de mes données, euh, je ne vais pas chercher forcément à me révolter (...) parce que j'ai un peu le sentiment d'un tonneau des Danaïdes. » (#5)

2.3. Formes de compétences collectives pour la protection de la vie privée

Nous relevons **2 formes de compétences collectives** (illustrée dans le Tableau 47 ci-dessous) :

- Les bénéfices sociétaux (Son & Kim, 2008), i.e., le degré selon lequel un utilisateur perçoit que sa plainte pour violation de sa vie privée en ligne pourrait bénéficier à d'autres utilisateurs en leur évitant d'être victime de la même manière.

Alors que Son & Kim (2008) montrent que les bénéfices sociétaux de la plainte influencent uniquement les plaintes, nos résultats suggèrent que les bénéfices sociétaux motivent tous types d'actions et tous types de personnes. En effet, les répondants déclarent (i) utiliser des moyens techniques de protection pour eux-mêmes mais également pour rendre ces moyens de protection actifs et disponibles pour d'autres, (ii) développer bien sûr des actions sociales dans le but de protéger un bien commun, (iii) mobiliser des actions institutionnelles pour rendre le droit vivant et réel. Le concept de bénéfices sociétaux fait pleinement référence aux théories des lanceurs d'alerte (*whistleblowing*), indiquant que les dénonciations faites par des employés concernant de mauvaises pratiques managériales proviennent essentiellement d'une volonté de protéger d'autres salariés des mêmes mauvaises pratiques (Dozier & Miceli, 1985).

- La protection du groupe, qui correspond aux fonctions de besoins de sécurité et de coopération des groupes sociaux d'appartenance.

Face à une violation de données personnelles, le groupe va jouer un rôle protecteur, pour trouver appui, pour se protéger, pour pouvoir dénoncer sans être menacé d'être responsable (e.g., hacker éthique inculqué ou lanceurs d'alerte) ou pour trouver de l'aide dans le cas de recours ou de plaintes collectives. Cette nécessité de protection du groupe est encore plus grande dans le cas de violations de données personnelles.

*

En conclusion, les compétences collectives sont pour le groupe (bénéfices sociétaux) et par le groupe (protection du groupe). De plus, dans le cas d'une violation de données personnelles majeure, la résignation (fatigue) et la nécessité du collectif (force et protection du groupe) sont encore plus prégnantes.

Tableau 47 : Formes de compétences collectives

Formes de compétences collectives	Verbatims illustratifs
Bénéfices sociétaux	« c'est un investissement que tu ne fais pas pour toi, uniquement, mais que tu fais aussi pour les autres. Parce que tu crois en cette valeur (...) cette nécessité de la protection pour toi, mais aussi pour les autres. Et donc du coup, c'est quelque chose que tu fais aussi pour les autres et pour quelque part, l'intérêt général » (#2) « On ne parle même plus de droits individuels (...) quand je passe des heures, parce que c'est clairement des heures et des jours à remplir des plaintes et des dossiers et des choses comme ça, à se battre, ce n'est même pas pour moi. Moi, c'est déjà sécurisé (...) Mais par contre, ouais, protéger les autres et se battre contre ces boîtes-là, empêcher que Bouygues ou Cdiscount revendent l'intégralité de ses bases clients, ben c'est ça aussi le but, quoi » (#8) « l'importance de porter à la connaissance de la CNIL ces choses-là, c'est mon droit individuel et le droit collectif, quoi » (#12 » « Ben pour pas que ça se reproduise pour moi, mais je me dis que si on est plusieurs à faire ça, euh, ça permettra peut-être aussi de faire évoluer les pratiques » (#1) « Les personnes qui cherchent par un moyen ou par un autre à être actives sur ces questions de protection des données personnelles ont des moteurs collectifs » (#9)
Protection du groupe	« On a un moyen très individualisé et qui je pense, pour ceux qui ont une attention particulière, ça ne répond pas du tout à la demande. Donc peut-être qu'on a besoin, pour certains (...) d'être un peu suractifs parce que pour pouvoir combler ce manque de vision collective sur la gestion des données personnelles. » (#9) « ben je préviens la CNIL (...) Le problème, c'est que (...) si tu es particulier (...) Il faut être vachement précautionneux, parce que tu peux être accusé d'avoir fait le coup (...) Donc j'ai vraiment porté le lundi à l'ANSSI ce problème-là (...) Moi-même, je ne sais pas trop quoi faire des fois » (#4) <u>Situation de violation de données personnelles de la CNAM :</u> « Peut-être qu'il y aura des plaintes collectives (...) Mais je ne vois même pas ce que je peux faire dans une situation pareille. Parce que c'est des cas tellement énormes qu'on se dit « Ben, je suis un peu démuni, en fait, face à ça ». (...) Peut-être que je ferais une plainte à la CNIL ou quelque chose comme ça et si j'entends parler qu'il y a des recours collectifs, ouais, enfin, des plaintes collectives, euh, j'essaierais peut-être de la rejoindre, mais en fait, c'est tellement énorme entre guillemets que quand ça nous tombe dessus, on est un peu abasourdi. Je ne sais même pas si je saurais quoi faire, enfin, qu'est-ce que je peux faire concrètement à part déposer plainte pour la forme, que ça soit individuellement ou collectivement ? Enfin, qu'est-ce que je peux faire à mon échelle pour que ça ait un impact pour ça ? » (#10) « Je hurle (rires), mais qu'est-ce que je peux faire ? Qu'est-ce que je peux faire ? Je ne peux rien faire. Au niveau individuel, je ne peux rien faire » (#12) « je pense que je porterais plainte à la CNIL (mais ...) je demanderais surtout à des gens que je connais en ligne qui sont un peu plus du coup calés là-dedans qu'est-ce que je peux faire comme démarches parce qu'il y a pleins de gens qui, bon... » (#10)

Section 6. Discussion et implications

Cette dernière partie permet de résumer les principaux résultats de notre recherche et de les mettre en perspective en identifiant ses contributions théoriques (1) et ses implications managériales (2). Nous concluons en identifiant les limites et les voies de recherche (3). Certains points sont développés et approfondis dans le chapitre 7 du manuscrit (discussion).

Dans cette recherche, nous montrons plusieurs résultats :

- **la défense d'une équité sociale** (i.e., le désir que chaque individu ait les mêmes droits et opportunités, indépendamment des différences sociales, du sexe, de l'origine, de la religion ou de la vulnérabilité) est une motivation essentielle pour l'activation d'actions de protection des données personnelles. Les personnes agissent dans une volonté d'équité sociale face à des inégalités dans les compétences techniques (notamment les compétences pour la protection de la vie privée) ou dans le besoin de confidentialité (cacher ses vulnérabilités étant plus important pour les plus vulnérables). Pour ce faire, ces personnes agissent (i) par des actions techniques pour elles-mêmes et en rendant ces moyens de protection actifs et donc accessibles à tous, (ii) en recourant à l'application de la loi (e.g., plaintes CNIL) pour elles-mêmes ou de manière plus collective. (iii) Et, elles développent des actions de soutien et de formation pour protéger le bien commun général ;
- Deux valeurs motivationnelles secondaires sont également identifiées : (i) **la liberté** (de choix, permettant à chacun de garder son jardin secret par des moyens techniques ou réglementaires) et directement liée à l'équité sociale (e.g., « *Ma propre liberté m'intéresse peu si elle n'est pas partagée par tout le monde* » (#9)) ; (ii) **la sécurité** ;
- De plus, la protection de la vie privée doit être envisagée comme une **pratique sociale**, reposant sur des dynamiques collectives : les individus agissent pour des raisons collectives et par des moyens collectifs. Si la protection des données personnelles est bien un droit individuel, elle ne peut être exercée individuellement, mais collectivement. Ceci est d'autant plus vrai dans le cas d'une grave violation de données personnelles : « tous pour un, un pour tous », un individu seul est impuissant face à une violation majeure de données ;

- **Ces pratiques sociales se développent autour de structures** mobilisant valeurs motivationnelles (i.e., idéaux qui incitent à l'action), compétences et croyances, et matériaux. Si les valeurs sont un puissant moteur de motivation pour être engagé dans la protection de ses données personnelles, elles se heurtent souvent à un manque de moyens techniques (i.e., outils de protection ergonomiques et accessibles), à des compétences limitées (i.e., alphabétisation numérique), à un sentiment limité d'efficacité personnelle, ou encore à de la résignation et de la lassitude. Ce déséquilibre entre valeurs motivationnelles, matériel disponible et compétences entrave le développement des pratiques efficaces de protection de la vie privée. À l'inverse, le développement d'un savoir (articulé autour de compétences, littératie et conscience des risques) et de pouvoir (par le développement d'outils techniques accessibles et de collectifs permettant la formation, l'entraide et le soutien), minimise l'importance des idéaux et des valeurs.

1. Contributions théoriques

Notre recherche apporte deux principales contributions théoriques (liées entre elles) aux recherches actuellement en cours sur la protection de la vie privée et des données personnelles.

1.1. Approche de la protection de la vie privée par la théorie de la pratique

Notre recherche envisage la protection de la vie privée comme une pratique sociale et offre un éclairage sociologique novateur, en dehors de cadres macro (institutionnels et économiques) ou micro (psychologiques).

La préoccupation pour la protection des données personnelles, i.e., la possibilité pour un individu de contrôler l'utilisation potentielle par des tiers de ses données personnelles (Belanger et al., 2002 ; Westin, 1967), repose sur un paradigme d'individualisme méthodologique (Boudon, 1984, 2002), i.e., un principe d'explication des phénomènes sociaux centrés sur les agents humains individuels. Ainsi, les phénomènes sociaux collectifs sont expliqués uniquement comme étant la somme des phénomènes et actions individuels. De fait, les principales théories mobilisées dans les recherches en vie privée reposent sur une compréhension où l'agent est au centre de tous les phénomènes : e.g., la théorie de l'agence ou la théorie du contrat social. Ces explications théoriques sont fondatrices des grands outils

réglementaires de la protection des données personnelles : e.g., le consentement, le droit de retrait, le droit d'effacement.

De plus, l'individualisme méthodologique a beaucoup été utilisé en économie, incluant une certaine forme de rationalité de la part des agents. L'agent observé dans les recherches en protection de vie privée est un *homo economicus*, faisant un calcul coût-bénéfice (dévoilement d'une partie de ses données personnelles et de son intimité vs. obtention d'un service personnalisé) dans les transactions concernant ses données personnelles. Même si le principe de régulation individuelle du partage de ses données personnelles (*self-data management*) a beaucoup été critiqué (Solove, 2020), considérant qu'il existe un trop fort décalage entre un comportement d'auto-divulgence dans un contexte donné et un désir de vie privée motivé par des idéaux et des valeurs, les nouvelles propositions théoriques restent centrées sur l'agent et l'individu. Les dernières théories prises en compte dans les recherches en vie privée (Li, 2012 ; Martin & Murphy, 2017) s'orientent vers des approches en psychologie (e.g., protection motivation theory, social cognitive theory) mais gardent une approche centrée sur un agent économique rationnel.

À notre connaissance, aucun éclairage sociologique considérant la préoccupation pour la protection de la vie privée comme un phénomène sociologique, un objet à part entière, indépendamment des agents n'a été à ce jour apporté. Ceci est assez étonnant alors que la vie privée, indépendamment de toute considération numérique ou digitale, a souvent été expliquée comme un phénomène sociologique (Schwartz, 1968), résultant d'une adaptation à un contexte donné, comme un vie nomade, ou des logements exigus (Ariès & Duby, 1985). De fait, notre recherche complète les précédentes recherches.

1.2. Remise en question d'une préférence à l'individualisme dans le cadre de la protection de la vie privée

Notre recherche confirme qu'une préférence culturelle pour l'équité sociale est une motivation essentielle aux actions de protection de la vie privée, contrairement à de très nombreuses recherches qui cherchent à établir un lien entre individualisme et protection de la vie privée (e.g., Miltgen & Peyrat-Guillard, 2014). Elle remet en question l'importance de l'individualisme comme valeur fondatrice du droit à la protection de la vie privée. Pour cela, il nous paraît intéressant de distinguer individualisme culturel et individualisme méthodologique. En effet, il existe une polysémie dans le terme « individualisme » (Chazel, 1991) et en sociologie, le terme d'individualisme sert à la fois à identifier un phénomène social (i.e., un système de valeurs reposant sur une préférence pour l'autonomie et l'atteinte des objectifs personnels, composante majeure des sociétés occidentales) et une démarche méthodologique (i.e., une façon d'appréhender les problèmes et la réalité).

De plus, l'approche par l'individualisme limite le développement du collectif et ancrer la protection des données personnelles dans des actions individualistes peut être la base d'un obstacle à la révolte collective. Nous approfondissons ce point dans le chapitre 7 (théorie de la pratique, effets d'engagement et de résistance). En effet, si la prise de parole (protestation) n'est pas la seule issue possible en cas de mécontentement, elle n'est pas non plus la plus simple (Hirschman, 1970) et elle représente des risques (temps nécessaire à prendre la parole, coût financier de la prise de parole, stigmatisation sociale) : elle a besoin de s'appuyer sur la force du nombre et la protection du groupe. Or pour cela, il faut que les individus aient conscience qu'ils ont intérêt à lutter ensemble dans l'objectif d'un bien commun. Comme la vie privée est identifiée comme un bien individuel, sans présenter les risques collectifs d'une violation des données de chacun, le bien commun reste peu identifié : les individus choisissent l'option de la loyauté (i.e., le fameux « tout le monde s'en fout »). Les options seraient (i) soit de diminuer le temps et le coût de la prise de parole (facilité des procédures) (ii) soit de montrer que l'intérêt collectif est plus important que l'intérêt individuel (e.g., à travers des normes subjectives).

D'autre part, comprendre la protection de la vie privée comme une pratique sociale structurelle permet de minimiser l'importance des idéaux au bénéfice des matériaux et compétences. Les orientations en matière de protection des données personnelles dans des pays comme l'Inde, la Chine et d'autres pays émergents (Martin & Murphy, 2017) peut s'expliquer par d'autres facteurs comme la distance psychologique, l'alphabétisation numérique, la self-efficacy ; tout

en gardant en mémoire que ces pays sont surtout animés d'un souhait d'indépendance post-colonial et mesurent le prix de leur indépendance et de leur sécurité.

2. Implications pratiques

Nous renvoyons le lecteur vers le chapitre 7 pages 362 à 376 pour une présentation détaillée des implications managériales de l'ensemble de notre travail, présenté dans le cadre général de la théorie de la pratique.

3. Limites et voies de recherches

Cette recherche présente bien sûr certaines limites qui sont autant de possibilités de recherches ultérieures :

- Nous pourrions compléter notre recherche par des informations complémentaires permettant une triangulation des données et une plus grande approche épistémologique et méthodologique de la compréhension d'une pratique sociale de la protection de la vie privée, plus centrée sur la pratique en elle-même que sur l'individu (agent) ;
- Nous pourrions compléter le nombre de personnes interrogées pour une validation empirique quantitative, et notamment pour permettre d'établir des chaînes moyens-fins (nécessitant une cinquantaine d'entretiens, cf. page 239) ;
- En faisant cela, nous pourrions diversifier les profils des personnes interrogées, notamment en termes d'engagement sur la protection de la vie privée (e.g., interroger plus de personnes agissant au sein d'organisations, d'entreprises et de collectivités territoriales).

Synthèse de l'essai 2

Notre deuxième recherche a pour objectif d'observer avec une approche qualitative à un niveau méso l'influence des normes socio-culturelles sur le comportement de réponse face à une violation de données personnelles.

Cette recherche confirme d'une part que la défense d'une équité sociale est une motivation essentielle à un engagement pour le respect de la vie privée, et, d'autre part, que la protection de la vie privée est une pratique sociale. Cette dernière se développe autour de structures mobilisant des valeurs (idéaux), des moyens (matériaux), et des formes de compétences (e.g., sentiment d'efficacité). Un développement équilibré entre idéaux, moyens et formes de compétences permet l'adoption d'une réponse active face à une violation de données personnelles. Enfin, les défenses de sa liberté ou de sa sécurité individuelle sont deux motivations supplémentaires à ces réponses.

Cette recherche offre un éclairage théorique novateur à la question de la protection de la vie privée : premièrement, elle l'envisage comme une pratique sociale, et non comme une pratique individuelle, éliminant l'idée que les individus sont les seuls responsables. Deuxièmement, elle remet en question la primauté de l'individualisme comme valeur fondatrice de la protection des données personnelles.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

Protection
des données
personnelles

Réponses des
consommateurs
insatisfaits

Culture
et valeurs



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :
Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :
Influence des
normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :
Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 6. Essai 3 - Influence des orientations culturelles individuelles sur le comportement de réponses face à une violation de données personnelles



Résumé de l'essai

Depuis l'entrée en vigueur du Règlement Général sur la Protection des Données personnelles (RGPD), le nombre de plaintes relatives aux violations de données personnelles varie fortement d'un pays à l'autre, interrogeant de fait le rôle de la culture dans les réactions des consommateurs en matière de protection de leur vie privée. Ainsi, cet article explore les mécanismes psychologiques reliant les préférences culturelles individuelles aux réponses comportementales face à une violation de données personnelles. Plus particulièrement, il interroge l'influence de la distance psychologique avec la violation de données personnelles. En utilisant l'échelle des orientations culturelles individuelles de Sharma (2010) et à l'aide d'une enquête conduite en France (N=452), nous montrons que certaines orientations culturelles, comme l'égalité sociale et l'égalité de genre, impliquent moins de distance psychologique avec la violation de données personnelles et peuvent favoriser des réponses techniques concrètes, tandis que d'autres orientations, comme l'indépendance, n'encouragent que la préoccupation pour la protection de ses données personnelles.

Biographie de l'essai

Une communication extraite de ce chapitre a été présentée à la Conférence Atlas-AFMI 2022 (Nice, France, du 3 au 5 mai), au Congrès de l'afm 2022 (Tunis, Tunisie, du 18 au 20 mai) et à la conférence EMAC 2022 (comme poster ; Budapest, Hongrie, du 24 au 27 mai).

Section 1. Introduction et fondements de la recherche

1. Introduction

Alors que les violations de données personnelles, i.e., la perte ou le vol d'informations personnelles confidentielles (Romanosky et al., 2011), entraînant des risques tels que la fraude bancaire, l'usurpation d'identité, la manipulation comportementale, sont en forte augmentation et touchent tous les pays, la protection des données personnelles devient une préoccupation centrale dans nos sociétés, amenant entre autres à la mise en place de réglementations comme le RGPD. Cependant, les pays européens diffèrent grandement dans le nombre de plaintes déposées auprès des autorités en charge de la protection des données personnelles. Entre mai 2018 et janvier 2021, le Danemark a enregistré 155,6 plaintes pour violation de données personnelles pour 100.000 personnes, contre 127,8 pour l'Irlande, 50,0 pour l'Allemagne et 2,8 pour la France¹¹⁷. Cette observation conduit à interroger l'influence de la culture sur la réponse à la violation de données personnelles.

Jusqu'ici, la littérature s'est principalement intéressée à la préoccupation pour la protection de la vie privée et à ses antécédents individuels, contextuels et culturels (Smith et al., 2011). Si elle met en évidence une influence claire de la culture sur la préoccupation pour la protection de la vie privée, elle marque des contradictions dans le sens cette influence pour certaines sous-dimensions de la culture, qui pourraient s'expliquer par une exploration insuffisante des mécanismes psychologiques en jeu et, de fait, appellent à davantage de recherches (Martin et al., 2020). Précisément, cette recherche aborde deux questions.

Premièrement, quelles sont les valeurs culturelles susceptibles d'expliquer la réponse à la violation de données personnelles ? Les recherches utilisent majoritairement le modèle de la culture nationale d'Hofstede (2001), et notamment les dimensions d'individualisme (préférence pour les intérêts individuels plus que ceux de la communauté), de distance hiérarchique (acceptation d'un ordre hiérarchique au sein de la société) et de masculinité (préférence pour l'action et le pragmatisme). Milberg et al. (2000) comme Bellman et al. (2004) montrent que ces trois dimensions influencent significativement la préoccupation pour la protection de la vie privée, mais dans des directions opposées. De plus, alors que beaucoup de recherches indiquent

¹¹⁷ DLA Piper GDPR fines and data breach survey. *op. cit.*

une plus grande préoccupation pour la protection de la vie privée par les individus vivant dans des pays valorisant l'individualisme, Lowry et al. (2011) observent que des étudiants chinois sont plus préoccupés par la protection des données personnelles que des étudiants américains plus individualistes. Ces constats démontrent que les niveaux de mesure des dimensions culturelles utilisées doivent être remis en question, car ils mesurent mal les caractéristiques culturelles individuelles (Oyserman et al., 2002). Dans une perspective individuelle et psychologique (Sharma, 2010), notre recherche propose de s'intéresser à l'influence des préférences culturelles individuelles.

Deuxièmement, une meilleure compréhension des mécanismes psychologiques à l'œuvre dans les réponses des consommateurs face à une violation de leurs données personnelles est nécessaire. Si des travaux ont exploré l'influence des violations de données personnelles sur les performances boursières des entreprises (e.g., Rasoulzadeh et al., 2021), leur impact sur le comportement du consommateur n'a été que très peu étudié (e.g., Labrecque, 2021). Son & Kim (2008) ont construit une taxonomie des réponses pour la protection de la vie privée et défini le rôle de trois antécédents à ces réponses (préoccupation pour la protection et le contrôle des données personnelles, justice perçue, bénéfices sociétaux). Parmi eux, préoccupation pour la protection et le contrôle des données personnelles (Belanger et al., 2002), influence tous les types de réponses pour la protection de la vie privée, jouant un rôle central dans le modèle. Plus récemment, Labrecque (2021) confirme le rôle de préoccupation pour la protection des données personnelles dans les mécanismes de réponses des consommateurs face à une violation de leurs données, en identifiant l'importance de la violation perçue du contrat social : la violation perçue du contrat social consiste en la violation de l'accord implicite entre une entreprise et ses clients de protéger les données personnelles confiées, reposant sur le principe de droit au contrôle de ses données personnelles. Or la préoccupation pour la protection et le contrôle des données personnelles intègre de multiples facettes et niveaux de compréhension probablement appréhendés différemment selon les cultures (Li et al., 2022). Il est possible que cette préoccupation soit un facteur moins important que d'autres facteurs dans les mécanismes de réponse, compte tenu du fait qu'il s'agisse d'un concept abstrait (Hallam & Zanella, 2017). D'autres médiateurs peuvent, également, influencer la réponse du consommateur à la violation de ses données.

C'est pourquoi, nous interrogeons le rôle médiateur de la distance psychologique avec la violation de données personnelles, i.e., l'influence de la représentation mentale que chacun se

fait d'une violation de données personnelles. En effet, Bandara et al. (2021) ont récemment démontré le rôle modérateur de la distance psychologique entre les préoccupations en matière de protection de la vie privée et les comportements défensifs (sans les préciser). La théorie des niveaux de représentation (Trope & Liberman, 2010) décrit la relation entre distance psychologique et niveaux d'abstraction dans la représentation mentale d'événements et analyse comment un individu parcourt mentalement des distances pour se représenter un événement : « La distance psychologique fait référence à la perception du moment *où* un événement se produit, *du lieu où* il se produit, *de la personne* qui vit ou subit cet événement, et *de la possibilité* qu'il se produise ou non » (Trope & Liberman, 2010, p.4).

La théorie des niveaux de représentation est pertinente pour notre sujet car les valeurs ont un impact plus important sur la représentation de construits abstraits (Eyal et al., 2009) tels que la préoccupation pour la vie privée (Bandara et al., 2018 ; Hallam & Zanella, 2017) : en raison de leur nature abstraite, les valeurs ont un impact plus important sur les intentions pour une situation future lointaine (Eyal et al., 2009). Enfin, très peu de recherches ont exploré la relation entre la culture et le niveau de représentation mentale et d'abstraction (Wiesenfeld et al., 2017), même si les contextes culturels et les valeurs déclenchent des schémas cognitifs (Hong et al., 2000; Shapira et al., in Fiske & Macrae, 2012, p.229-250) et jouent un rôle clé dans les représentations mentales (Oyserman et al., 2002 ; Shapira et al. 2012). Mobiliser la théorie des niveaux de représentations pour étudier l'influence d'effets culturels pourrait faire apparaître des résultats novateurs.

Notre recherche adresse, de ce fait, la question : quels sont les mécanismes psychologiques en jeu dans l'influence des valeurs culturelles individuelles sur les réponses des individus face à une violation de leurs données personnelles ? Pour y répondre, nous appliquons la théorie des niveaux de représentation pour la première fois au cas des violations de données personnelles, et nous étudions les effets médiateurs de la distance psychologique avec les violations de données personnelles et de la préoccupation pour la protection des données, entre les orientations culturelles individuelles et les réponses face à une violation de données personnelles. Ces réponses peuvent être techniques (e.g., protéger techniquement ses informations personnelles), soit sociales (i.e., parler autour de soi ou sur les réseaux sociaux de la violation de données), soit institutionnelles (i.e., porter plainte à l'autorité nationale de protection des données personnelles et demander réparation). Concrètement, nous nous demandons par exemple si une préférence pour l'indépendance et l'autonomie provoque un

souci important de protection de son intimité et de contrôle de ses données et par conséquent l'usage d'outils informatiques protecteurs (e.g., VPN) ? Ou bien encore si une aversion culturelle au risque rend anxieux et donc plus concrète et plus probable une possible violation de données générant ainsi des habitudes de protection et de plaintes ?

Pour ce faire, nous avons mené une enquête en ligne auprès de 452 Français et analysé les résultats selon la méthode des équations structurelles. Notre recherche confirme le rôle central de la distance psychologique dans les mécanismes reliant valeurs culturelles et réponses face à une violation de données personnelles. Elle révèle également que les orientations culturelles ont un impact différent sur chaque type de réponse de protection de la vie privée. Certaines orientations culturelles, comme une préférence pour l'égalité sociale et l'égalité des genres, impliquent moins de distance psychologique avec les violations de données personnelles et peuvent favoriser des réponses techniques concrètes, tandis que d'autres, comme une préférence pour l'indépendance, n'encouragent que les préoccupations pour la protection des données personnelles et favorisent des réponses sociales ou institutionnelles.

Cette recherche apporte des contributions théoriques pertinentes (e.g., en proposant des éléments pour la construction d'une échelle de distance psychologique avec les violations de données personnelles). Elle expose également des pistes pour améliorer les politiques et actions de protection de la vie privée, en identifiant les leviers d'action psychologiques utiles pour activer les types de réponses, afin de protéger la vie privée en ligne de chacun, quelles que soient ses valeurs culturelles.

2. Fondements théoriques

Dans cette partie, afin d'éviter toute répétition avec des éléments conceptuels précédemment énoncés dans les chapitres précédents (essentiellement chapitres 1 et 2), nous indiquons uniquement les points essentiels des fondements théoriques de notre recherche et les paragraphes à consulter pour des développements plus complets.

2.1. Violations de données personnelles et réponses de protection du consommateur

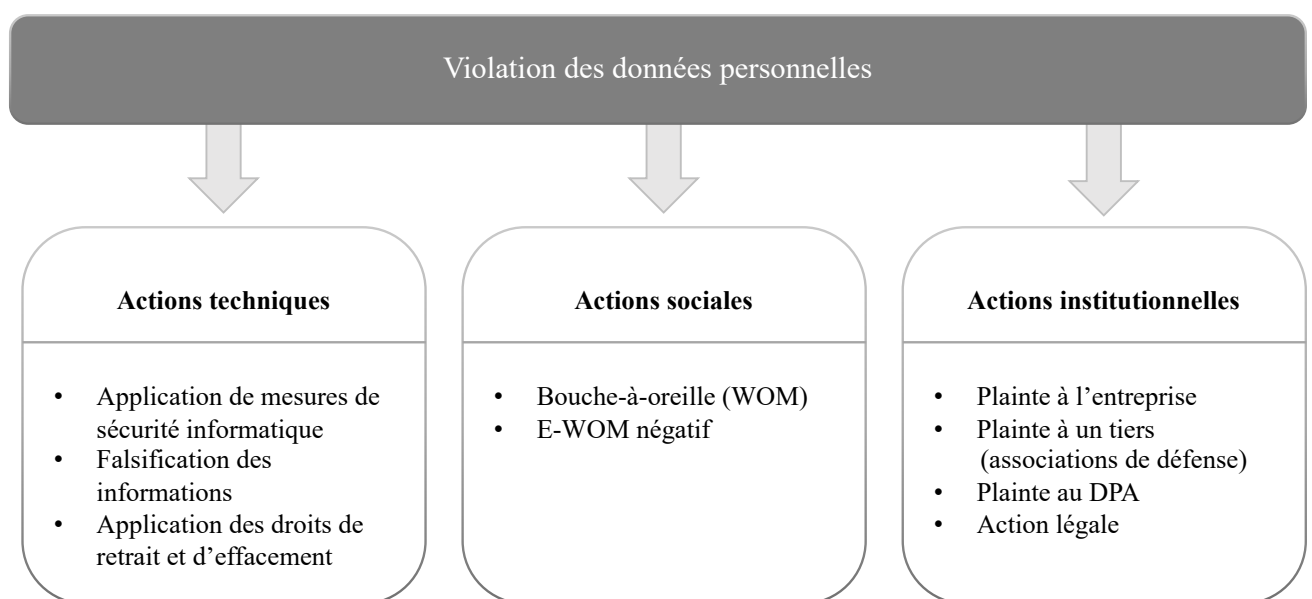
2.1.1. *Définition des violations de données personnelles*

Nous renvoyons aux pages 5 et 6 du manuscrit (introduction générale) pour la définition des violations de données personnelles.

2.1.2. *Réponses aux violations de données personnelles*

Nous renvoyons au chapitre 2 (section 2 – pages 121 à 125) pour plus d'explications concernant les réponses aux violations de données personnelles. Pour mémoire, nous présentons de nouveau la typologie des réponses possibles dans la Figure 38 ci-dessous.

Figure 38 : Typologie de réponses face à une violation de données personnelles



2.1.3. Mécanismes psychologiques à l'œuvre dans la réponse face à une violation de données personnelles

Le comportement de réponse face à une violation de données personnelles semble mobiliser les mêmes processus que le comportement classique de plainte du consommateur (Labrecque, 2021; Son & Kim, 2008). Il dépend :

- Du niveau d'insatisfaction générée par la violation,
- De l'objectif attribué à la résolution (e.g., résoudre le problème, diminuer l'émotion),
- De la justice perçue et des bénéfices sociétaux d'une réponse (Son & Kim, 2008),
- Du coût de la réponse et de la probabilité perçue de succès,
- Et enfin d'un processus cognitif-émotif (Lazarus, 1966, 1991), composé notamment du stress généré par l'insatisfaction de service (d'autant plus important que le service non satisfait porte sur des éléments privés et intimes ; Labrecque, 2021) et qui influence la perception du consommateur et son évaluation de la situation.

Le comportement de réponse des consommateurs face à une violation de données personnelles et les mécanismes psychologiques qui y sont à l'œuvre sont encore très peu explorés (Labrecque, 2021). Son et Kim (2008) ont toutefois identifié trois antécédents saillants : la préoccupation pour la protection des données personnelles, la justice perçue, les bénéfices pour la société. La préoccupation pour la protection des données personnelles influence tout type de réponses, jouant ainsi un rôle central, alors que les bénéfices pour la société n'influencent que le comportement de plainte, et la justice perçue n'influence que les réponses individuelles de protection des données. Plus récemment, Labrecque (2021) identifie la perception de violation de contrat social (i.e., la violation de l'accord implicite entre le consommateur et l'entreprise de l'existence d'un droit de contrôle sur ses données, opérationnalisé notamment par les obligations de consentement) comme mécanisme important de réponse et place ainsi la préoccupation pour la protection des données personnelles comme un construit majeur dans les réponses apportées par les consommateurs face à une violation de leurs données personnelles.

2.2. Préoccupation pour la protection des données personnelles

Nous renvoyons au chapitre 2 (section 1 – pages 87 à 100) pour les développements conceptuels de la préoccupation pour la protection de la vie privée et le souci de contrôle de ses données personnelles (*information privacy concern*).

Dans le cadre de cet essai, nous soulignons uniquement les interrogations en cours sur son rôle dans les décisions des consommateurs. En effet, les recherches sur la psychologie de la vie privée et la formation des préoccupations des consommateurs en matière de protection de la vie privée sont principalement basées sur le modèle APCO (Antecedent - Privacy Concern - Outcomes ; Smith et al., 2011 ; Dinev et al., 2015). Le modèle APCO donne à la préoccupation pour la protection de la vie privée (*information privacy concern*) une place centrale entre antécédents (individuels ou contextuels) et résultats (*outcomes* ; divulgation ou non des données).

Néanmoins, le principe d'autonomie et de responsabilisation des consommateurs vis-à-vis de leurs données personnelles, tout comme le rôle central de la préoccupation pour la protection de la vie privée, est remis en question. D'une part, il existe un paradoxe de la vie privée, i.e., un écart entre les préférences déclarées pour la protection de la vie privée mais distantes et abstraites (Bandara et al, 2018), et le comportement réel en termes de divulgation de la vie privée (Pavlou, 2011), qui privilégie des solutions en ligne plus concrètes. D'autre part, si le concept de la préoccupation pour la protection de la vie privée a été développé dans un contexte de sollicitation relativement contrôlée des données personnelles (e.g., marketing direct ou mailing postal), il soulève des questions face à l'explosion des données, à l'utilisation du Big data et de l'intelligence artificielle (Dignum, 2019), aux techniques de publicité ciblée ou de suivi en ligne subreptice (Martin & Murphy, 2017), et à l'effet boîte noire de la collecte de données (e.g., vendeur en ligne invisible, suivi non déclaré ; Pasquale, 2015). Les techniques actuelles de collecte et d'usage des données personnelles rendent les consommateurs moins conscients de cette collecte de données, moins autonomes et plus vulnérables (Martin et al., 2017).

Il en résulte que la préoccupation pour la protection de la vie privée est un concept abstrait (Bandara et al., 2018; Hallam & Zanella, 2017), et plusieurs recherches ont mobilisé la théorie de la distance psychologique pour éclairer les comportements paradoxaux lors des arbitrages liés à la vie privée. Nous les détaillons dans la partie suivante.

2.3. Distance psychologique et préoccupations pour la protection des données personnelles

2.3.1. Théorie de la distance psychologique

Parce que l'être humain est capable de se projeter et de s'imaginer des situations en dehors de celle qu'il vit à un instant présent, plusieurs chercheurs se sont intéressés au concept de distance psychologique (ou perspective psychologique), définie comme « *les différentes difficultés associées à l'atteinte d'un état final* » (Travers, 2015, p 3). Il s'agit de comprendre les conséquences liées à la représentation d'événements futurs (positifs ou négatifs) qu'une personne cherche à éviter ou non (i.e., conception « approche-évitement » des événements ; Miller, 1944). Cette conception « approche-évitement » peut générer des erreurs ou des réussites dans la réalisation de différentes tâches (e.g., Buehler et al., 1994), que la recherche en psychologie cherchait à expliquer. Or il manquait un cadre conceptuel pour éclairer ces questions, auquel Trope & Liberman (2010) répondent.

La théorie des niveaux de représentation (Trope & Liberman, 2010) analyse comment un individu peut aller au-delà de son expérience immédiate (le soi – *self* – ici et maintenant) et parcourir des distances mentalement pour représenter un objet. La théorie repose sur l'idée que plus la distance avec un objet ou un événement est importante, plus celui-ci sera abstrait : plus une distance psychologique augmente, i.e., la distance entre moi (ici et maintenant) et un événement, plus le niveau d'abstraction (de l'événement ou de l'objet) augmente. À l'inverse, plus la distance diminue, plus l'événement ou plus l'objet sera perçu comme concret.

La distance psychologique comprend 4 dimensions : temporelle, spatiale, sociale et hypothétique. En d'autres termes : « la distance psychologique fait référence à la perception *du moment où* un événement se produit, *du lieu où* il se produit, *de la personne pour qui* il se produit et *du fait qu'il* se produit ou non » (Trope & Liberman, 2010, p.4). Ces quatre distances sont corrélées (Fiedler et al., 2012) et interdépendantes : la distance sociale affecte et est affectée par les distances spatiale et temporelle (Stephan et al., 2010), ces deux dernières étant considérées comme des distances de base (Boroditsky & Ramscar, 2002).

Enfin, la distance psychologique est un concept différent de la distance psychique culturelle, i.e., la distance perçue entre deux pays ou deux cultures (Håkanson & Ambos, 2010), concept notamment développé en management international.

2.3.2. *Distance psychologique et consommation*

La distance psychologique est utilisée en marketing pour activer certains leviers et favoriser certains types de réponses du consommateur. Par exemple, Amazon joue sur la distance temporelle en mettant en avant la rapidité de ses livraisons pour activer l'acte d'achat, tandis qu'Hermès, tout en mobilisant aussi la distance temporelle, va mettre en avant un délai long de disponibilité de ses produits pour activer le sentiment de rareté et d'exclusivité d'un sac à main et favoriser l'acte d'achat (Didi Alaoui & Cova 2021) (cf. Tableau 48). La distance psychologique est également mobilisée en marketing et comportement du consommateur pour expliquer les différences d'efficacité publicitaire (e.g., entre des messages en *News Feed page* et en *Timeline page* sur Facebook ; Kim et al., 2016), l'impact du cadrage d'un message sur les intentions d'achat d'un produit innovant (Balbo & Jeannot, 2015), les différences d'évaluation de services clientèle (entre un service client en face à face ou un service clientèle à distance ; Hartley & Green, 2017), les réticences à effectuer des achats en ligne (Darke et al., 2016).

Certains travaux ont montré le rôle de la distance psychologique dans la relation entre culture et efficacité marketing. Ainsi, les individus « collectivistes » préfèrent les publicités montrant des produits ou services proches dans le temps (distance temporelle basse) et détaillées avec des informations concrètes (permettant d'éviter toute erreur risquant de perturber l'équilibre de la communauté), alors que les individus « individualistes » sont intéressés par l'effet long terme (distance temporelle élevée) du service et du produit, permettant de visualiser l'atteinte des objectifs, même s'ils restent abstraits (Kim et al., 2018).

Tableau 48 : Dimensions de la distance psychologique et applications dans un contexte de consommation (Didi Alaoui & Cova 2021)

Dimensions	Définitions	Sous-type	Contextes d'utilisation (ex.)
Temporelle	Intervalle de temps entre le jugement, l'évaluation ou le choix d'un objet et le moment où l'objet donné se réalise	Distance temporelle passée Distance temporelle future	Consommation d'un produit ou service dans un passé proche vs. lointain Livraison d'un produit dans un futur proche vs. lointain
Spatiale	Espacement physique existant entre un individu et un objet donné	Distance spatiale conceptuelle (imaginer de la distance physique entre soi et un <i>stimulus</i>) Distance spatiale perceptuelle (percevoir de la distance physique entre soi et un <i>stimulus</i>)	Choix ou consommation dans un lieu proche vs. éloigné du domicile du consommateur Proximité vs. éloignement physique entre le consommateur et les <i>stimuli</i> présentés
Sociale	Distinction qu'une personne fait entre elle-même et les autres	Le soi La similarité Le groupe La culture La politesse Le pouvoir	Achat pour soi vs. un ami Choix ou don en lien avec une personne similaire vs. dissimilaire Distinction entre personnes de l'endogroupe vs. exogroupe Activation du soi interdépendant vs. indépendant Tutoiement vs. vouvoiement Pouvoir fort vs. faible
Hypothétique	Probabilité d'occurrence d'un événement ou d'une situation	Degré d'incertitude Degré de réalité	Probabilité forte vs. faible de la réalisation d'un événement <i>Stimuli</i> réels vs. fictifs

2.3.3. Distance psychologique et préoccupation pour la protection des données personnelles

Plusieurs recherches novatrices (cf. Tableau 49) prennent appui sur la théorie de la distance psychologique pour éclairer le paradoxe de la vie privée (i.e., le décalage entre les intentions déclarées de protection de la vie privée et les comportements réels de divulgation de données personnelles ; Pavlou, 2011). La préoccupation pour la protection des données personnelles étant un construit distant et abstrait (Lutz & Strathoff, 2014), ayant pour conséquence qu'un risque éloigné paraît peu probable, son rôle est moins important dans les interactions en ligne

(qui nécessitent la divulgation de données) que la satisfaction ou les récompenses obtenues immédiatement (Bandara et al., 2020 ; Cloarec et al., 2022 ; Hallam & Zanella, 2017). Ainsi, « en raison de la distance spatiale, temporelle, sociale et hypothétique des valeurs associées à la vie privée, celle-ci est interprétée comme un phénomène abstrait influençant la formation d'attitudes et d'intentions dans un avenir lointain plutôt que le comportement réel » (Bandara et al., 2018, p.2).

Ces recherches indiquent que le souci de protection de la vie privée influence principalement les intentions de protection de la vie privée (Hallam & Zanella, 2017), et non les intentions de divulgation de données. Ceci s'explique par le fait que les transgressions (violations de vie privée) qui se produisent dans des situations psychologiquement éloignées ont des implications morales plus fortes que les transgressions immédiates (Bandara et al., 2018). Bandara et al. (2020) complètent la compréhension du paradoxe de la vie privée comme étant le résultat non seulement de la distance psychologique, mais également d'une résignation et d'un sentiment d'impuissance des individus quant à la protection de leur vie privée suite à de multiples violations. Enfin, Bandara et al. (2021) valident empiriquement le concept de distance psychologique avec la préoccupation pour la protection de la vie privée. Selon eux, la distance psychologique affaiblit aussi la relation entre préoccupations en matière de vie privée et comportement défensif, et que les personnes autonomes et compétentes en matière de vie privée ne sont pas influencées dans leurs intentions comportementales par la distance psychologique avec la vie privée.

Par ailleurs, alors que Hallam & Zanella (2017) ne considèrent que la distance temporelle, sans en préciser les raisons, Bandara et ses collègues (2018, 2020, 2021) prennent en considération les 4 dimensions hypothétique, sociale, spatiale et temporelle de la distance psychologique. Ainsi, chez Bandara et al. (2018), la préoccupation relative à la protection des informations personnelles est :

- Très hypothétique (« Je pense que le risque que cela [les atteintes à la vie privée] se produise réellement est assez faible. Il faut être raisonnablement malchanceux pour que cela vous arrive », p.3682) ;
- Éloignée dans l'espace (« ce n'est pas comme si vous voyiez quelqu'un avec une arme à côté de vous, c'est un problème invisible. Donc, ce n'est pas comme si on le leur rappelait à chaque achat », p.3682) ;

- Socialement distante (« cela [les violations de la vie privée] n'est pas arrivé à beaucoup de gens [que je connais]. Mes amis et ma famille n'ont pas été affectés par cela. Si quelque chose arrive à mes amis ou à ma famille, si j'entends parler de quelque chose qui s'est produit, alors je serais inquiet », p.3683) ;
- Éloignée dans le temps (« vous pouvez en bénéficier [des avantages] immédiatement, alors que pour la vie privée, ce n'est peut-être pas certain », p.3683).

À notre connaissance, aucune recherche n'a auparavant mobilisé la théorie des niveaux de représentation en croisant culture et préoccupation pour la protection de la vie privée. Pourtant, cette approche nous semble prometteuse pour faire progresser la recherche.

Tableau 49 : Distance psychologique et préoccupations pour la protection de la vie privée

Auteurs	Points clés
Hallam & Zanella (2017)	Les activités sur les réseaux sociaux proches dans le temps (concrètes) réduisent dans les choix quotidiens le poids des risques de violation de la vie privée éloignés dans le temps (pas encore expérimentés et psychologiquement éloignés).
Bandara et al. (2018)	Parce que la vie privée et ses valeurs sont éloignées hypothétiquement, spatialement, socialement et temporellement (par ordre décroissant d'importance) et interprétées comme un phénomène abstrait, elles influencent la formation d'attitudes et d'intentions lointaines plutôt que le comportement réel et proche et la prise de décision directe pour la protection de la vie privée.
Bandara et al. (2020)	Cet article éclaire le paradoxe de la vie privée en utilisant trois thèmes : la distance psychologique de la vie privée, le contrat social perçu en matière de protection de la vie privée, et l'autonomisation apprise en matière de protection de la vie privée.
Bandara et al. (2021)	Cette recherche valide empiriquement le concept de distance psychologique avec la préoccupation pour la protection de la vie privée, et montre d'une part que la distance psychologique affaiblit la relation entre préoccupations en matière de vie privée et comportement défensif, et d'autre part que les personnes autonomes et compétentes en matière de vie privée (<i>empowered</i>) ne sont pas influencées dans leurs intentions comportementales par la distance psychologique avec la vie privée.

2.4. Culture et orientations culturelles individuelles

2.4.1. Culture et valeurs culturelles

Ce paragraphe reprend quelques idées clés concernant la culture que nous avons détaillées au chapitre 2 (section 3 – pages 126 à 154).

La culture est une construction collective, un ensemble des solutions et d'éléments explicites et implicites développés par chaque groupe social (Matsumoto, 2007), et permettant de vivre ensemble (Schein, 2015). Elle résulte de l'adaptation des êtres humains à leur environnement (Matsumoto, 2007). Ainsi culture est, en ce sens, « un ensemble complexe qui comprend les connaissances, les croyances, l'art, la morale, la coutume et toutes les autres capacités et habitudes acquises par l'homme en tant que membre de la société » (Tylor, 1871, p.1). Souvent représentée à travers la métaphore de « l'oignon » (Hofstede, 1997), cette structure en couches constitue un continuum entre éléments explicites de la culture ou artefacts (e.g., la langue, la nourriture, les vêtements, les rites, les institutions, les lois) et éléments subjectifs et implicites, à savoir les valeurs ou les normes (Schein, 1984). Ce point est détaillé dans cette recherche.

Les valeurs résultent à la fois de l'héritage culturel, reçu pendant l'enfance, et d'expériences personnelles (Rokeach, 1973). Elles sont universelles (Schwartz, 1992, 2006), différenciées individuellement (Trompenaars, 1996) et évoluent sur une longue échelle de temps (Inglehart, 2018). Un système de valeurs est une organisation apprise de principes et de règles pour aider une personne à choisir entre des alternatives, à résoudre des conflits et à prendre des décisions, une tendance à préférer certaines situations à d'autres (Rokeach, 1973), basée sur le principe qu'un mode de conduite ou un état final d'existence est préférable à un autre. Les valeurs sont, de ce fait, des construits abstraits et constituant un ordre éthique pour chacun.

2.4.2. Modèles de mesures des valeurs culturelles

Au cours des 60 dernières années, les anthropologues et les chercheurs en management interculturel ont essayé de comprendre et de représenter les éléments subjectifs et invisibles de la culture, à travers la définition de valeurs et dimensions (e.g., Hofstede, 1984, 2001; Hofstede et al., 2010; Inglehart & Welzel, 2005; Kluckhohn & Strodtbeck, 1961; Rokeach, 1973; Schwartz, 1992, 2006).

Parmi ces modèles, le modèle des dimensions de la culture nationale d'Hofstede est le plus utilisé dans les recherches en management international et en marketing international (de Mooij, 2017), notamment pour étudier l'influence de la culture sur le comportement de plainte des consommateurs (Zhang et al., 2008). Néanmoins, de nombreux chercheurs (e.g., Ailon, 2008; Jones, 2007; Livian, 2011), dont Hofstede lui-même, indiquent que les dimensions culturelles au niveau national ne peuvent pas être utilisées au niveau individuel car tous les individus d'un même pays n'ont pas exactement les mêmes orientations culturelles individuelles (Oyserman et al., 2002). L'application des échelles nationales au niveau individuel pose donc problème (Brewer & Venaik, 2012).

En vue d'« individualiser » les dimensions d'Hofstede, Sharma (2010) propose une échelle de 40 items qui mesurent dix orientations culturelles au niveau individuel. La richesse de l'échelle de Sharma réside :

- Avant tout dans sa multidimensionnalité, permettant de mesurer les orientations culturelles à un niveau individuel d'une manière fiable à travers différentes cultures. Pour cela, Sharma (2010) complète les dimensions d'Hofstede avec d'autres perspectives culturelles, permettant de nuancer les différences individuelles dans les orientations culturelles ;
- Dans sa robustesse, l'échelle ayant été testée dans différents contextes internationaux (i.e., Hong Kong, Royaume-Uni, USA, Chine, Inde) renforçant de fait sa validité d'équivalence interculturelle ;
- Cette échelle permet de couvrir les différentes dimensions culturelles tout en restant condensée, en comparaison par exemple avec les échelles de Schwartz (Schwartz, 2006; Schwartz et al., 2012).

Cette multidimensionnalité apporte plus de nuances sur les orientations. Ainsi si certaines orientations sont proches (e.g., inégalité sociale et indépendance), elles expriment chacune des subtilités suffisamment précises pour écarter toute possibilité de corrélation entre elles (ou de hiérarchisation de niveaux). En particulier, Sharma (2010 ; cf. p792) a construit son échelle en excluant tout item reflétant une attitude générale ou une ambiguïté de sens.

Finalement, la correspondance entre les dimensions de la culture nationale d'Hofstede et al. (2010) et les orientations personnelles de Sharma (2010) nous aide à lier conceptuellement nos différents chapitres empiriques, comme expliqué ci-après.

2.4.3. *Définitions des grandes orientations culturelles*

Dans ce paragraphe, nous reprenons à nouveau les dimensions d'Hofstede (précédemment détaillées page 68, mais uniquement dans l'objectif d'établir leurs correspondances avec les orientations culturelles de Sharma (2010).

Hofstede (Hofstede, 1984, 2001; Hofstede et al., 2010) identifie 6 dimensions de la culture nationale (i.e., distance hiérarchique, individualisme, masculinité, contrôle de l'incertitude et orientation à long terme, indulgence) et Sharma (2010) 10 orientations culturelles individuelles (pouvoir et inégalité sociale, indépendance et interdépendance, masculinité et égalité des sexes, aversion au risque et intolérance à l'ambiguïté, tradition et prudence). Les 5 premières dimensions d'Hofstede et les 10 orientations de Sharma se correspondent comme suit (cf. Tableau 50) (la dimension « indulgence » n'est pas mobilisée, probablement car elle est ajoutée en 2010 par Hofstede, année de publication de l'échelle de Sharma).

A) Distance hiérarchique : La dimension de distance hiérarchique d'Hofstede (1980) est définie comme le degré selon lequel les membres les moins puissants d'une société acceptent et s'attendent à ce que le pouvoir soit distribué de manière inégale : elle intègre deux éléments de pouvoir et d'égalité. Afin de permettre une distinction claire de ces éléments, Sharma propose deux orientations culturelles : l'inégalité sociale (qui définit la relation des personnes à l'égalité sociale et le degré selon lequel un individu accepte l'inégalité entre les membres d'un groupe social) et le pouvoir (qui définit la relation des personnes à l'autorité et le degré selon lequel les individus acceptent des différences de pouvoir entre les membres d'un groupe social).

B) Individualisme : La dimension d'individualisme d'Hofstede (1980) s'entend comme une préférence pour un cadre social dans lequel les individus s'occupent essentiellement d'eux-mêmes et de leur famille proche, par opposition à la dimension de collectivisme. Considérant que ces deux dimensions ne sont pas uniquement les deux extrêmes d'un même continuum (Oyserman, 2006) et que chaque individu possède en lui une double tendance vers un souci d'individualisme (pour l'atteinte de ses objectifs personnels) ou de collectivisme (pour le souhait de partager des buts et des normes communs avec d'autres) (Triandis et al., 1985), Sharma reconceptualise ces dimensions en deux orientations culturelles personnelles : l'indépendance et l'interdépendance.

L'indépendance et l'interdépendance représentent différentes manières d'envisager la construction de soi et ne sont pas corrélées négativement. L'indépendance représente une préférence pour une construction de soi autonome et individuelle alors que l'interdépendance représente une préférence pour une construction de soi au sein d'un groupe social. Une même personne peut avoir une double vision de soi (e.g., des membres de groupes alternatifs dont chaque membre est indépendant vis-à-vis de la société ou de ses proches mais interdépendant avec son groupe identitaire). En outre, ces visions de soi peuvent être influencées par le contexte culturel (Markus & Kitayama, 1990) : une vision de soi indépendante peut être moins admise dans des pays à orientation collectiviste et traditionnelle.

C) Masculinité : La dimension de masculinité d'Hofstede (1980) se caractérise comme une préférence dans la société pour l'accomplissement, l'héroïsme et l'affirmation de soi (par opposition à la coopération, la modestie, le souci des faibles et la qualité de vie), reconceptualisé par Sharma (2010) en deux dimensions : (i) la masculinité (i.e., la préférence pour l'affirmation de soi et la confiance en soi, pouvant se traduire par de l'agressivité et de l'ambition), et (ii) l'égalité des genres (i.e., la préférence pour l'harmonie sociale, l'humanité, l'égalité entre hommes et femmes, que ce soit en termes de rôles sociaux, de capacités, de droits et de responsabilités).

D) Contrôle de l'incertitude : Sharma (2010) a reconceptualisé la dimension de contrôle de l'incertitude d'Hofstede (1980), définie comme le degré selon lequel les membres d'une société se sentent mal à l'aise face à l'incertitude et à l'ambiguïté, en deux dimensions : l'aversion au risque (i.e., le degré selon lequel les individus sont réticents à prendre des risques ou à prendre des décisions risquées) et l'intolérance à l'ambiguïté (i.e., le degré selon lequel les individus acceptent l'ambiguïté et les situations incertaines).

E) Orientation à long terme : La dimension d'orientation à long terme d'Hofstede (1980) est, quant à elle, une préférence pour le pragmatisme pour préparer l'avenir plus que pour les traditions ancestrales et les normes strictes, « l'encouragement de vertus orientées vers les récompenses futures, en particulier la persévérance et l'épargne » (Hofstede, 2001, p.359) ; alors qu'une orientation court terme se focalise sur le respect des traditions, la stabilité, la sauvegarde des apparences (Donthu & Yoo, 1998). Hofstede a ajouté cette dimension pour une meilleure représentation des sociétés orientales et asiatiques, et les normes éthiques attachées au confucianisme. Or cette définition génère une confusion sur la compréhension du respect des traditions : s'agit-il d'une valeur à court ou long terme ? Cette confusion est peut-être due

aussi à une mauvaise connaissance du confucianisme. C'est pourquoi Bearden et al. (2006) redéfinissent l'orientation à long terme comme « la valeur culturelle d'une vision holistique du temps, qui valorise à la fois le passé et l'avenir, plutôt que de considérer les actions comme importantes uniquement pour leurs effets dans l'immédiat ou à court terme ». Bearden et al. (2006) définissent également deux sous dimensions qui sont ensuite reprises par Sharma (2010) : (i) la tradition (i.e., une préférence pour le respect des valeurs traditionnelles, telles que le travail acharné, le non-matérialisme, la bienveillance, la conscience sociale, la moralité et le respect de l'héritage), et (ii) la prudence (i.e., une préférence pour la planification, la persévérance, l'épargne et l'orientation vers l'avenir). Ces deux dimensions sont positivement corrélées.

Tableau 50 : Définitions des orientations culturelles de Sharma (2010)

Dimensions de la culture nationale d'Hofstede	Orientations culturelles individuelles de Sharma	Définition
Distance hiérarchique	Inégalité sociale	Définit la relation des personnes à l'égalité sociale et le degré selon lequel un individu accepte l'inégalité entre les membres d'un groupe social
	Pouvoir	Définit la relation des personnes à l'autorité et le degré selon lequel les individus acceptent des différences de pouvoir entre les membres d'un groupe social
Individualisme vs. collectivisme	Indépendance	Préférence pour l'indépendance, la liberté individuelle, l'autonomie et l'accomplissement personnel, associée à une forte représentation de son <i>soi</i> et de son individualité, et amenant à une préférence pour l'accomplissement, la réussite, la compétence et la satisfaction des plaisirs
	Interdépendance	Préférence pour le sentiment d'appartenance à un ou plusieurs groupes sociaux, la conformité à l'identité de groupe, l'importance accordée aux objectifs du groupe, l'accomplissement collectif et la confiance dans les autres
Masculinité	Masculinité	Préférence pour la maîtrise et l'affirmation de soi, la confiance en soi, pouvant se traduire par de l'agressivité et de l'ambition
	Égalité des genres	Préférence pour l'harmonie sociale, l'humanité, l'égalité entre hommes et femmes, que ce soit en termes de rôles sociaux, de capacités, de droits et de responsabilités
Contrôle de l'incertitude	Aversion au risque	Le degré selon lequel les individus sont réticents à prendre des risques ou à prendre des décisions risquées
	Intolérance à l'ambiguïté	Le degré selon lequel les individus acceptent l'ambiguïté et les situations incertaines
Orientation à long terme	Tradition	Préférence pour le respect des valeurs traditionnelles, telles que le travail acharné, le non-matérialisme, la bienveillance, la conscience sociale, la moralité et le respect de l'héritage
	Prudence	Préférence pour la planification, la persévérance, l'épargne et l'orientation vers l'avenir

Section 2. Modèle conceptuel et développement des hypothèses

1. Distance psychologique et préoccupation pour la protection de la vie privée

1.1. Application de la distance psychologique aux violations de données personnelles

Le souci de protection de la vie privée est un construit abstrait et lointain (e.g., Bandara et al., 2018; Hallam & Zanella, 2017), très hypothétique, éloigné dans le temps et l'espace et socialement distant. La théorie des niveaux d'abstraction a été utilisée pour mesurer la distance (hypothétique, temporelle, sociale et spatiale) avec le risque de violation de la vie privée. Par exemple : « cela [les violations de la vie privée] n'est pas arrivé à beaucoup de gens [que je connais] », (Bandara et al., 2018) ; ou encore « au moment de faire des achats en ligne, à quel point le concept de vie privée est-il éloigné dans votre esprit ? (de très proche à très éloigné) », (Bandara et al., 2021).

Nous suggérons d'appliquer la théorie de la distance psychologique aux cas de violations de données personnelles. En effet, l'élément déclencheur du comportement de réponse est la violation de données personnelles : la distance psychologique avec la violation de données personnelles peut éclairer les mécanismes psychologiques de réponses aux violations.

De plus, réduire la distance psychologique a été identifié comme un levier efficace pour activer des réponses et des actions de prévention face au réchauffement climatique (Brügger et al., 2016; De Guttery et al., 2017; Singh et al., 2017; Spence et al., 2011, 2012) ou l'adoption d'une alimentation saine (Ronteltap et al., 2012). Une meilleure compréhension de la distance psychologique avec la violation de données personnelles peut permettre d'identifier des pistes d'actions intéressantes.

De ce fait, nous mobilisons la distance psychologique avec la violation de données personnelles, i.e., la perception de *quand*, *où*, *à qui* et *si* une violation de données personnelles peut se produire.

1.2. Préoccupation pour la protection des données personnelles et distance psychologique avec la violation de données personnelles

L'élément déclencheur du processus de plaintes et de réponses face à une violation de données personnelles est le niveau d'insatisfaction générée par cette violation (e.g., Olivier, 1997) : il y a insatisfaction parce qu'une attente n'a pas été confirmée. Le niveau d'insatisfaction dépend ainsi de la compréhension de la situation : comment être insatisfait si ce qui s'est produit nous paraît normal ? Comment être insatisfait si nous ne comprenons pas ce qui vient de se produire ?

Par exemple, dans le cas de l'alimentation saine, Ronteltap et al. (2012, p.334) indiquent que « pour bien comprendre la valeur de la santé pour les consommateurs, il est de la plus haute importance de savoir comment les consommateurs interprètent le concept de santé ». Or, la préoccupation pour la protection de la vie privée est un concept abstrait (e.g., Bandara et al., 2018), dont la compréhension peut varier selon les pays, les cultures, et les groupes sociaux.

Comprendre les mécanismes psychologiques reliant orientations culturelles et réponses face à une violation de données personnelles consiste, selon nous, à répondre à deux questions :

- Comprendre comment chacun se représente l'objet de la violation (le *what*), à savoir le droit de contrôler l'accès à l'usage de ses données personnelles (Belanger et al., 2002) et la préoccupation pour la protection de ses données personnelles ;
- Comprendre comment chacun se représente les moyens de la violation (le *how*), à savoir la distance psychologique avec qui sépare chacun du phénomène de violation de données personnelles.

En d'autres termes, deux construits sont des médiateurs dans la relation qui lie les orientations culturelles individuelles et les réponses des consommateurs face à une violation de leurs données personnelles : la préoccupation pour la protection de ses données personnelles et la distance psychologique avec la violation de données personnelles (Bandara et al., 2021). Ces deux construits favoriseront la compréhension des mécanismes psychologiques, et de facto les orientations culturelles en jeu ainsi que les types de réponses apportées.

Par ailleurs, la préoccupation pour la protection de ses données personnelles et la distance psychologique avec la violation de données personnelles sont liés. Il en est de même dans le cas du changement climatique : le changement climatique est un construit psychologiquement distant (Spence et al., 2012) et les individus qui estiment peu probables les impacts du

changement climatique (distance hypothétique) ou qui estiment que les impacts toucheront des personnes éloignées (distances spatiale et sociale) sont moins susceptibles d'être préoccupés par les impacts du changement climatique (Singh et al., 2017). Plus le changement climatique est concret et proche psychologiquement, plus la préoccupation pour le changement climatique est importante (Brügger et al., 2016).

Enfin, plus l'importance donnée à la vie privée pour les individus est élevée, plus leurs perceptions de la violation de la vie privée dans un contexte de commerce électronique sont élevées (Rejikumar et al., 2021). En raison de l'aspect abstrait du concept de préoccupation pour la protection de données personnelles, nous postulons que la relation est inverse. Nous supposons que plus un individu perçoit une violation de données comme un événement abstrait, moins il est préoccupé en matière de protection des données personnelles.

H1 : la distance psychologique avec la violation de données personnelles influence négativement la préoccupation pour la protection des données personnelles

2. Influence des orientations culturelles individuelles

2.1. Influence de l'indépendance

La préoccupation pour la protection de sa vie privée est en lien avec l'indépendance. Un souci individuel de protection de sa liberté et de son autonomie résulte de façon évidente dans un souci de protection de la vie privée ; et une vision de soi indépendante implique une vision autour du secret et de la discrétion. Les précédentes recherches se sont essentiellement intéressées au lien entre l'individualisme et le souci de protection de la vie privée, montrant généralement qu'une préférence pour l'individualisme favorise la préoccupation pour la protection de la vie privée en ligne et limite la divulgation d'informations personnelles (Dinev et al., 2006; Milberg et al., 2000; Muk, 2007; Posey et al., 2010; Steenkamp & Geyskens, 2006). En effet dans les pays qui valorisent l'individualisme, les gens croient que chacun a le droit de défendre sa vie privée (Milberg et al., 2000), tandis que dans les pays où l'individualisme est moins important, on accepte davantage les pratiques organisationnelles qui empiètent sur la vie privée (Smith et al., 1996). De la même manière, nous émettons l'hypothèse qu'une préférence

personnelle pour l'indépendance favorisera la préoccupation pour la protection des données personnelles.

Par ailleurs, l'information peut être traitée différemment selon les préférences culturelles. Une vision indépendante de soi est associée à des représentations mentales abstraites d'événements futurs et à la perception que ces événements se produisent dans un avenir plus lointain : la perception mentale est logique, analytique et orientée vers le résultat (elle est alors faiblement contextualisée). À l'inverse, une vision interdépendante de soi est associée à des représentations concrètes d'événements futurs et à la perception de ces événements comme se produisant dans un avenir plus proche : la perception mentale nécessite de recevoir des informations de base et contextuelles pour être comprises, elle est fortement contextualisée (Spasova & Lee, 2013). Ces différentes façons d'interpréter l'information avec des orientations soit indépendantes (orientées vers la disposition) soit interdépendantes (orientées vers le contexte) sont respectivement associées à des interprétations de haut et bas niveau (Kim et al., 2018). Une préférence pour l'indépendance favorise donc la représentation mentale de concepts abstraits, telle que la préoccupation pour la protection des données : plus je suis indépendant, plus je suis préoccupé pour la protection de la vie privée.

H2a : l'indépendance influence positivement la préoccupation pour la protection des données personnelles

Plus précisément, la manière de traverser des distances mentalement est culturellement différente. Le processus cognitif de représentation, de construction et de hiérarchisation mentales (Hong et al., 2000; Vallacher & Wegner, 1989) nécessite de « s'orienter dans l'espace, de planifier l'avenir, d'apprendre du passé, de se rapporter et de comprendre les autres » (Trobe & Liberman, 2010, p.4). Les réflexes cognitifs influencent notre représentation séquentielle des événements : « les gens construisent spontanément des représentations mentales de séquences d'événements liées temporellement et thématiquement » (Chiu & Hong, 2007, p.792), et les liens de causalité entre plusieurs événements sont essentiellement temporels (Baudet, 1990). La relation au temps sous-tend toute projection mentale (Eyal et al., 2009). Parmi les différentes distances composant la distance psychologique, les distances temporelle et spatiale sont les deux distances de base (Boroditsky, 2000; Boroditsky & Ramscar, 2002). Or la relation au temps dans les sociétés industrialisées et majoritairement individualistes est orientée vers le futur dans un état de « fiction opératoire » (Bergadaa, 1990). Le temps est vu de façon *monochronique* (une tranche horaire = une action) et non *polychronique* (pas de tranches

horaires ou de division du temps, plusieurs actions en même temps) (Hall, 1976). Ceci amène les individus ayant une préférence pour l'indépendance à plus facilement se projeter abstraitement dans le temps et à parcourir la distance temporelle qui sépare le *self* et l'objet abstrait. Nous émettons alors l'hypothèse que plus un individu valorise l'indépendance, plus il sera en capacité de se représenter une violation de données personnelles, éloignée dans le temps.

En outre, les individus ayant une préférence pour l'indépendance n'hésitent pas à faire des choix ou à prendre des décisions indépendamment du reste du groupe. Si le groupe privilégie une préférence pour l'usage des réseaux sociaux ou le partage d'informations non sécurisées (à travers l'utilisation du réseau WhatsApp appartenant à Meta qui comptait 2 milliards d'utilisateurs actifs par mois en octobre 2021¹¹⁸), un individu indépendant n'hésitera pas à faire des choix contraires (en utilisant l'interface Signal ou Telegram, quitte à se couper d'une partie de son entourage). En revanche, les individus interdépendants ont tendance à éviter des comportements qui pourraient entraîner des perturbations sociales ou décevoir les autres (Heine et al., 1999). Ainsi, les personnes ayant des préférences pour l'interdépendance au groupe ont des attitudes plus positives à l'égard des événements temporellement proches en raison des informations détaillées et concrètes qui leur permettent d'éviter les erreurs. En revanche, les personnes ayant une préférence pour l'indépendance sont donc plus intéressées par l'état final souhaité du résultat que par les informations détaillées (Kim et al., 2018; Markus & Kitayama, 1990).

Pour finir, à la suite de notre première hypothèse (i.e., la distance psychologique avec la violation de données influence négativement les préoccupations pour la protection des données), nous émettons l'hypothèse que l'indépendance a un impact négatif sur la distance psychologique avec la violation de données personnelles : l'indépendance ayant une influence positive sur la préoccupation pour la protection des données, qui elle-même est corrélée négativement avec la distance psychologique, l'indépendance est corrélée négativement avec la distance psychologique avec la violation de données personnelles.

H2b : l'indépendance influence négativement la distance psychologique avec la violation de données personnelles

¹¹⁸ [https://www.proinfluent.com/chiffres-reseaux-sociaux/#:~:text=Aujourd'hui%2C%20WhatsApp%E2%84%A2%20se,Octobre%202021\)%%20%5B1%5D](https://www.proinfluent.com/chiffres-reseaux-sociaux/#:~:text=Aujourd'hui%2C%20WhatsApp%E2%84%A2%20se,Octobre%202021)%%20%5B1%5D).

2.2. Influence de l'inégalité sociale

Nous faisons ici le choix de regrouper sous le terme « inégalité sociale » l'ensemble des items afférents à l'inégalité sociale et au pouvoir, tels que définis par Sharma (2010).

Les personnes qui acceptent l'inégalité sociale, i.e., l'absence d'égalitarisme entre les personnes dans une société, acceptent également la discrimination (en fonction par exemple de l'âge, de la classe sociale, de la position professionnelle ; Yoo & Donthu, 2005). Or, la discrimination sociale implique d'avoir accès à des données personnelles (Petrescu et al., 2020) : le droit à la protection de la vie privée, tel qu'il est inscrit dans la Déclaration universelle des droits de l'homme de 1948, repose lui-même sur des faits de discrimination et a pour objectif de protéger les individus des excès de la Seconde Guerre mondiale (en particulier le fichage des personnes, l'ingérence de la police dans le domicile des personnes, la possibilité d'identifier des relations spécifiques, des préférences sexuelles ou des convictions politiques). Pour mémoire, la société Dehomag (DEutsche HOLLenrith-MASchinen Gesellschaft), à cette époque filiale d'IBM, avait permis d'identifier les juifs durant les années 30, ce qui facilita leur déportation dans les camps de concentration. Nous émettons l'hypothèse que les personnes ayant une préférence pour l'inégalité sociale sont moins préoccupées par la protection de la vie privée et des données personnelles.

De plus, les personnes qui acceptent les différences de pouvoir entre les membres d'un même groupe peuvent accepter de livrer une partie de leur vie privée à un autre, supérieur hiérarchiquement et plus autoritaire : ils ont donc une préoccupation pour la protection de leurs données personnelles moins importante. En effet, les cultures valorisant une forte distance hiérarchique connaissent une norme de contrôle et d'autorité plus formelle, qui s'accompagne d'un partage de l'information centralisé et restreint (Lowry et al., 2011). Il est admis que des informations personnelles soient connues (par exemple, partager son état de santé et ses feuilles de sécurité sociale avec son employeur) et qu'un contrôle social (avec utilisation des technologies) soit exercé. Ceci est conforme aux travaux de Bellman et al. (2004) ainsi que Cao & Everard (2008) qui ont trouvé une relation négative entre la dimension de distance hiérarchique (Hofstede, 1980) et la préoccupation pour la protection des données personnelles.

H3a : l'inégalité sociale influence négativement la préoccupation pour la protection des données personnelles

En outre, une étude récente (Madan et al., 2022) révèle qu'une distance hiérarchique élevée rend les utilisateurs plus enclins à penser qu'une violation de données personnelles est admissible. En effet, les personnes acceptant une hiérarchie sociale et une distribution du pouvoir inégale au sein d'une société pensent que les entreprises, et non elles-mêmes, sont propriétaires des données personnelles compromises. En raison de cela, ces personnes continuent à fréquenter une entreprise après une violation de données personnelles et ne réduisent pas leurs transactions avec l'entreprise. Le *how* et les fondements de la violation de données personnelles restent lointains et abstraits : nous en déduisons que plus les individus acceptent une inégalité sociale, plus les violations de données personnelles sont distantes psychologiquement.

H3b : l'inégalité sociale influence positivement la distance psychologique avec la violation de données personnelles

2.3. Influence de l'aversion au risque

Nous faisons ici le choix de regrouper sous le terme « aversion au risque » l'ensemble des items afférents à l'aversion au risque et à l'intolérance à l'ambiguïté, tels que définis par Sharma (2010).

Les personnes qui ne sont pas à l'aise avec la prise de risques essaient de se protéger contre tout risque, quel qu'il soit. Leurs perceptions des atteintes à la vie privée les renvoient à des préoccupations ou appréhensions concernant l'utilisation de leurs données personnelles (Rejikumar et al., 2021). Moins les personnes aiment prendre de risques, plus elles vont se préoccuper de la protection de leurs données personnelles. Ceci est conforme à des travaux précédents qui ont montré que des scores élevés de contrôle de l'incertitude (Hofstede, 1980) sont associés à des niveaux élevés d'anxiété, de stress et par conséquent de préoccupation pour la sécurité et pour la protection de la vie privée (Milberg et al., 1995 ; Smith et al., 1996).

De plus, l'intolérance à l'incertitude et à l'ambiguïté amène les individus à être vigilants sur la protection de leur vie privée. Comme ces personnes ont des doutes et ne sont pas certaines de ce que les autres font de leurs informations personnelles (par exemple sur les réseaux sociaux), elles vont être vigilantes sur ce qu'elles communiquent (par exemple en limitant le partage d'informations sur les réseaux sociaux) : l'évitement de l'incertitude a une incidence positive sur la sensibilité des utilisateurs aux relations interpersonnelles en ligne (Lowry et al., 2011).

Par ailleurs, la paranoïa est un trait de caractère fortement corrélé à la préoccupation pour la protection de la vie privée (Smith et al., 1996) : il est plausible que les personnes paranoïaques soient également susceptibles d'être plus préoccupées par la protection de leurs informations personnelles.

H4a : l'aversion au risque influence positivement la préoccupation pour la protection des données personnelles

De plus, l'anxiété face à l'avenir amène les individus à réduire la distance temporelle qui les sépare de certains événements : plus les individus sont psychologiquement anxieux face à l'incertitude de l'avenir, plus ils ressentent le besoin de diminuer cette incertitude et plus ils vont chercher à se représenter l'avenir, que celui-ci soit positif ou négatif (Urieu, 2000). Par ailleurs, les personnes étant en capacité d'abstraction ont une préférence pour le risque faible : ils font preuve d'abstraction pour se représenter un événement, ce qui les conduit à un comportement éthique (Zhang et al., 2022). Moins une personne aime prendre des risques, moins les violations de données personnelles sont abstraites pour cette personne.

En outre, une anxiété face à l'avenir et à son incertitude augmente le sentiment de probabilité qu'un événement peut se produire, et réduit la distance psychologique hypothétique. Ceci s'est illustré par exemple dans le cas de la crise sanitaire du Covid 19 : les personnes les plus culturellement anxieuses étaient celles qui pensaient que les risques liés à la maladie pouvaient être les plus importants et celles qui se protégeaient le plus (Ahmadi et al., 2022).

H4b : l'aversion au risque influence négativement la distance psychologique avec la violation de données personnelles

2.4. Influence de l'égalité des genres

Les recherches précédentes prennent peu en compte la dimension de masculinité d'Hofstede et dévoilent des résultats contradictoires et mitigés. Milberg et al. (1995) trouve un effet positif entre masculinité et préoccupation pour la protection des informations personnelles, tandis que Bellman et al. (2004) souligne que « les cultures à forte masculinité mettent davantage l'accent sur la réussite et le succès matériels, et peut-être sur les avantages économiques de l'utilisation d'informations privées, que sur les relations attentionnées et la qualité de vie » (Bellman et al.,

2004, p.315). Mais cette hypothèse n'est plus vérifiée par Lowry et al. (2011). Par voie de conséquence, nous excluons l'existence de lien entre une préférence pour l'affirmation de soi et l'ambition (masculinité) et la préoccupation pour la protection de la vie privée. Et parmi les deux orientations de Sharma (2010), seule l'égalité des genres nous semble avoir un lien avec la protection des données personnelles.

En effet, l'égalité des genres ne concerne pas seulement l'égalité juridique et sociale entre femmes et hommes, mais également une harmonie sociale dans son ensemble, qui passe par la défense de l'humanité et des droits fondamentaux. Les personnes ayant une préférence pour l'égalité des genres, ont une préférence pour la liberté et l'égalité de chacun. Ces personnes sont conscientes que combattre les inégalités, les discriminations et les vulnérabilités, c'est défendre protection de chacun et la liberté de tous. Or la protection de la vie privée et des données personnelles est un moyen important de protéger les risques de discriminations. Il en découle que les personnes ayant une préférence pour l'égalité des genres ont une préoccupation pour la protection de la vie privée.

H5a : l'égalité des genres influence positivement la préoccupation pour la protection des données personnelles

Par ailleurs, comme déjà souligné, certaines valeurs développent des dispositions à l'abstraction. Par exemple, le pragmatisme (valeur qui se rapproche de la masculinité) est une valeur qui varie culturellement et qui influence la capacité d'abstraction (Yetiser, 2015). La proximité temporelle (i.e., se focalisant sur le *here and now*) active le pragmatisme et une distance temporelle active l'idéalisme (Kivetz & Tyler, 2007). De plus, les caractéristiques individuelles influencent le rapport à la distance temporelle (Kim et al., 2018) et selon Nisan (1972), les individus orientés vers le succès sont plus susceptibles de renforcer les attentes de succès et de prise de risque lorsque la distance temporelle devient plus grande. Nous en déduisons que l'égalité des genres, comprise dans son orientation vers la masculinité, a un impact négatif sur la distance psychologique avec la violation de données personnelles.

H5b : l'égalité des genres influence négativement la distance psychologique avec la violation de données personnelles

2.5. Influence de l'orientation vers la tradition

Le registre culturel traditionnel comprend un répertoire de valeurs comme par exemple de la droiture, de la bénédiction, de la parole donnée (Bourqia, 2010) : ces valeurs sont souvent portées par la religion (Inglehart & Baker, 2000). Ainsi une orientation culturelle vers la tradition favorise la conscience sociale et morale : rendant ainsi la protection de la vie privée plus préoccupante. Une préférence culturelle pour la prudence favorise la sensibilité à l'impact à long terme de nos actions, et donc une plus grande préoccupation pour la protection de la vie privée (Krasnova et al., 2012; Trepte et al., 2017). Les deux sous-dimensions ont donc un effet positif sur la préoccupation pour la protection des données personnelles.

H6a : l'orientation vers la tradition influence positivement la préoccupation pour la protection des données personnelles

Cependant, une orientation culturelle vers la tradition inclut le respect de valeurs telles que le non-matérialisme, impliquant une vie quotidienne moins hyperconnectée et rendant les violations de données personnelles moins concrètes.

En outre, les individus valorisant une orientation vers la prudence et l'orientation holistique vers l'avenir appréhendent le changement, les oppositions et les paradoxes différemment. Par exemple, Peng & Nisbett (1999) soulignent que face à un conflit entre mères et filles, des étudiants chinois ont tendance à se concentrer sur la réconciliation de la contradiction en considérant le mérite et la faute des deux côtés (e.g. « les mères et les filles ont échoué se comprendre »), alors que les étudiants américains ont tendance à être en faveur d'une partie (e.g. « les mères doivent respecter l'indépendance des filles »).

Les individus valorisant la prudence sont habitués à gérer des situations paradoxales, comme le paradoxe entre le souci de la protection de la vie privée et la nécessité de communiquer ses données personnelles pour l'accès à certains services : ils vont chercher à concilier les deux. L'acceptation de ces contradictions conjuguées avec un travail dur sont des modes de fonctionnement acceptés auparavant au Japon et maintenant en Chine. En revanche, ces contradictions peuvent générer une dissonance cognitive (i.e., une incompatibilité entre deux états cognitifs et un décalage entre valeurs et comportements ; Chataigné, 2014; Heinich, 2017) et nous faisons l'hypothèse qu'un éloignement psychologique avec les risques associés aux

violations de données personnelles est nécessaire pour accepter cet état de dissonance. Ainsi une orientation vers la tradition rend plus abstraites les violations de données personnelles.

H6b : l'orientation vers la tradition influence positivement la distance psychologique avec la violation de données personnelles

3. Réponses face à une violation de données personnelles

Les personnes soucieuses de la protection de leur vie privée se soucient des pratiques des entreprises liées à l'utilisation de leurs données personnelles (Smith et al., 1996), et des conséquences importantes qu'une mauvaise utilisation de ces données peut avoir (Dinev et al., 2006). Ces personnes vont donc chercher à activer plusieurs types de réponses pour limiter les conséquences. Par ailleurs, des recherches précédentes ont montré que la préoccupation pour la protection de la vie privée influence principalement les comportements de protection des données personnelles (vs. les comportements de divulgation de données personnelles ; Smith et al., 2011) et tous les types de réponses de protection pour la protection des données personnelles (Son & Kim, 2008).

H7 : la préoccupation pour la protection de la vie privée influence positivement les réponses (a) techniques, (b) sociales et (c) institutionnelles

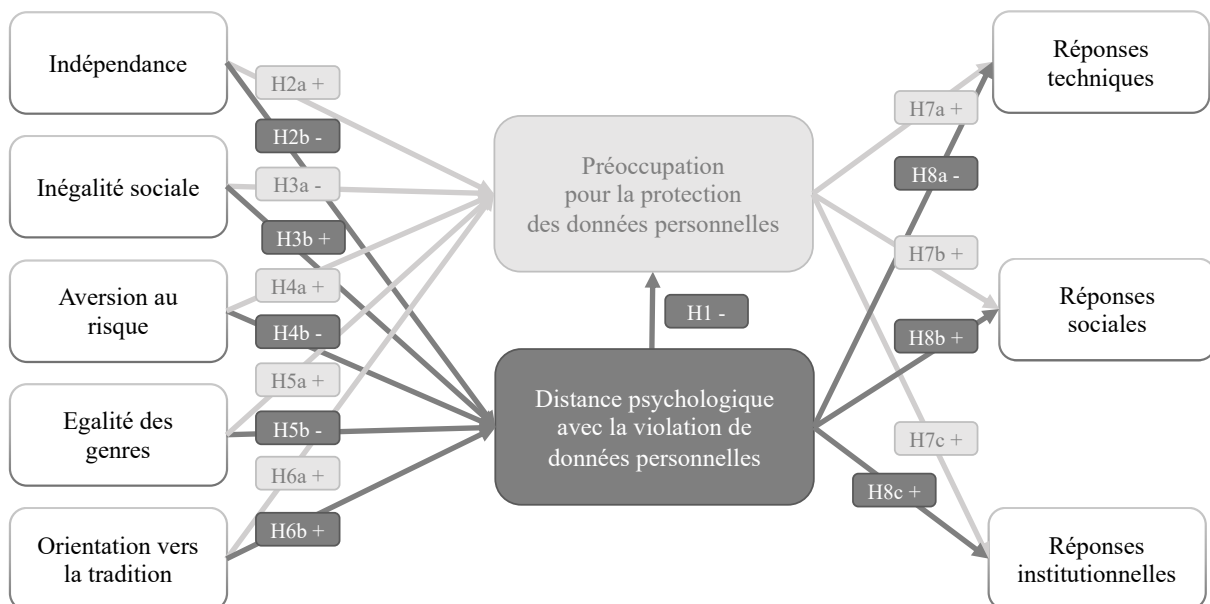
Plusieurs théories, comme la théorie de l'action raisonnée (Fishbein & Ajzen, 1980), la théorie du comportement planifié (Ajzen, 1991) et l'approche de l'action raisonnée (Fishbein & Ajzen, 2011) suggèrent que les intentions comportementales sont influencées entre autres par la force des croyances concernant les résultats du comportement effectué (i.e., si le résultat est probable ou non). Donc la distance hypothétique avec les violations de données va influencer les intentions comportementales face aux violations de données. En revanche, plus la distance hypothétique et psychologique va être importante, plus l'intention comportementale et éthique va être importante. En effet, les personnes ayant un niveau de construction élevé (par rapport à un niveau faible) sont plus susceptibles d'avoir l'intention de se comporter de manière éthique (Zang et al., 2022). Les questions morales, nécessitant des constructions mentales abstraites, attirent davantage les individus dans leur réflexion à distance que les choix de décision réels et immédiats (Bandara et al., 2021).

Enfin, si des recherches récentes soulignent que « la distance psychologique de la vie privée influence négativement le comportement de protection de la vie privée » (Bandara et al., 2021, p.1), il n'existe pas d'autres recherches à ce sujet. Nous nous attendons à ce que la distance psychologique avec la violation de données personnelles n'ait pas le même impact sur les réponses de protection de la vie privée : les plus autonomes, pour qui les violations de données sont concrètes, préféreront les réponses techniques, tandis que les plus démunis, pour qui les violations de données restent abstraites, se tourneront vers les réponses institutionnelles en en parlant.

H8 : la distance psychologique avec la violation de données personnelles influence (a) négativement les réponses techniques, et positivement (b) les réponses sociales et (c) institutionnelles.

La Figure 39 représente le modèle conceptuel de l'essai 3.

Figure 39 : Modèle conceptuel de l'essai 3 niveau Micro



Section 3. Recherche empirique et résultats

1. Méthodologie

Un questionnaire établi à partir d'échelles existantes a été administré à un panel de 452 répondants en France. Les données ont ensuite été analysées par la méthode des équations structurelles. Nous détaillons dans cette partie les choix effectués.

1.1. Choix des échelles

Nous avons établi un questionnaire sur la base d'échelles déjà existantes.

Les orientations culturelles individuelles sont mesurées à l'aide de l'échelle de Sharma (2010), dont nous avons gardé l'ensemble des 40 items. Nous utilisons l'échelle utilisée par Miltgen et al. (2016) pour mesurer la préoccupation pour la protection de la vie privée et l'adaptions à notre contexte.

Comme il n'existe pas d'échelle validée ni pour la mesure de la distance psychologique avec la vie privée (Bandara et al., 2021) ni pour la mesure de la distance psychologique avec les violations de données personnelles, nous avons utilisé plusieurs sources pour construire nos items : (i) nous avons utilisé l'échelle de Spence et al. (2012) développée dans le cadre du changement climatique (exemples d'items : « ma région est susceptible d'être affectée par le changement climatique » ; « je ne suis pas certain que le changement climatique se produira réellement ») et nous l'avons adaptée au cas des violations de données personnelles, (ii) nous avons ajouté les questions ouvertes utilisées par Bandara et al. (2018) dans le cadre d'une approche qualitative (exemples d'item : « par rapport à d'autres pays, quel est le niveau de protection de la vie privée en Australie ? »). Il est à noter qu'au moment de la construction du questionnaire, nous n'avons pas utilisé les items que l'échelle de Bandara et al. (2021) dont nous n'avions pas connaissance.

L'ensemble des items sont indiqués dans le Tableau 51.

Tableau 51 : Indices de validité réelle et de convergence

Reliability and convergent validity indices

SEM-PLS Model fit: Absolute GoF = 0,306
Internal GoF = 0,890 ; External GoF = 0,991

Absolute GoF = 0,320
Internal GoF = 0,854 ; External GoF = 0,994

		Résultats scénario 1 (piratage accès site Internet)			Résultats scénario 2 (piratage carte bancaire)		
Variable latente	Items	Cross-loadings	Reliability	Convergent validity	Cross-loadings	Reliability	Convergent validity
Indépendance	Je préfère compter sur moi-même que de dépendre des autres	0,839	0,853	0,659	0,839	0,853	0,660
	Il est important pour moi d'avoir mon identité personnelle, indépendante des autres	0,793			0,792		
	La plupart du temps, je compte sur moi-même plutôt que sur les autres	0,804			0,805		
Aversion au risque	Je préfère un mode de vie "routinier" à un mode de vie imprévisible plein de changements	0,838	0,876	0,643	0,839	0,877	0,644
	Je me décrirais comme quelqu'un qui ne prend pas de risques	0,878			0,876		
	Pour éviter de faire des erreurs, je n'aime pas prendre trop de risques	0,849			0,850		
	J'ai tendance à m'angoisser facilement quand je ne peux pas prévoir le résultat de mes actions	0,614			0,619		
Inégalité sociale	J'ai tendance à suivre les ordres sans poser de questions	0,788	0,795	0,565	0,787	0,795	0,565
	Il m'est difficile d'interagir avec des personnes d'un statut social différent du mien	0,701			0,702		
	J'accepte que toutes les personnes au sein d'une même société ne soient pas traitées de façon équitable et égale	0,763			0,763		
Egalité des genres	Il est tout à fait normal que les hommes soient parfois émotifs	0,710	0,803	0,505	0,710	0,803	0,505
	Les hommes ne sont pas obligés d'être le seul soutien au sein d'une famille	0,686			0,686		
	Les hommes peuvent prendre soin des autres autant que les femmes	0,668			0,667		
	Les femmes peuvent être aussi ambitieuses que les hommes	0,774			0,774		
Tradition	Je suis fier(e) de ma culture	0,552	0,863	0,687	0,556	0,863	0,688
	Pour moi, le respect des traditions est important	0,927			0,927		
	Les valeurs traditionnelles sont importantes pour moi	0,947			0,947		
Distance psychologique avec les violations de données personnelles	Les violations de données personnelles affectent principalement des pays qui se trouvent loin d'ici	0,821	0,834	0,626	0,819	0,834	0,626
	Les violations de données personnelles ne peuvent pas arriver à des personnes comme moi	0,744			0,742		
	La gravité des violations de données personnelles est exagérée	0,807			0,810		
Information privacy concern	Mes données personnelles sont partagées avec des tiers sans mon accord	0,852	0,869	0,625	0,864	0,867	0,622
	Mon comportement et mes activités en ligne peuvent être surveillés	0,768			0,757		
	Mes données personnelles en ligne sont utilisées pour m'envoyer des offres commerciales	0,714			0,702		
	Mon identité est reconstituée à l'aide de données personnelles provenant de différentes sources	0,820			0,822		
Réponses techniques	Je change mes codes d'accès au site Internet et mets un mot de passe sécurisé *	0,846	0,780	0,545	0,821	0,871	0,692
	Je contacte par téléphone et email le site Internet en question pour bloquer l'accès à mon compte en ligne *	0,711			0,879		
	Je contacte par email ou par téléphone le site Internet pour demander réparation *	0,642			0,794		
Réponses sociales	J'en parle à mes proches	0,808	0,817	0,690	0,633	0,766	0,628
	J'en parle sur les réseaux sociaux ou sur des blogs	0,853			0,925		
Réponses institutionnelles	Je contacte une association de protection des consommateurs ou un élu pour me défendre et obtenir réparation	0,860	0,928	0,764	0,860	0,911	0,721
	Je porte plainte à la CNIL (Commission Nationale Informatique et Libertés)	0,866			0,917		
	Je demande le soutien d'une association ou d'un avocat pour lancer une action en justice afin de demander réparation	0,903			0,929		
	Je porte plainte à la police	0,866			0,665		
Age	-	1,000	1,000	1,000	1,000	1,000	1,000
Tendance à la plainte	-	1,000	1,000	1,000	1,000	1,000	1,000
Privacy self-efficacy	En cas de violation de mes données personnelles, il me serait facile de réagir	0,907	0,917	0,847	0,914	0,917	0,847
	J'ai confiance dans ma capacité à réagir face à une violation de mes données personnelles	0,933			0,927		

* items pour scénario 1 légèrement différents de ceux du scénario 2 (e.g.: je change mes codes d'accès à ma banque en ligne et met un mot de passe sécurisé / Je contacte par téléphone ou email ma banque pour faire opposition à ma carte bancaire)

1.2. Construction de scénarios

Nous avons construit deux scénarios de violations de données :

- Scénario 1 : « Imaginez qu'un site Internet que vous fréquentez souvent (site marchand ou réseau social) vous annonce que vos coordonnées d'accès au site (identifiant et mot de passe) ont été piratées. Que faites-vous ? : pouvez-vous nous indiquer la probabilité que vous réalisiez chacune des actions suivantes, sur une échelle allant de 1 (« absolument pas probable ») à 7 (« très fortement probable ») ? »
- Scénario 2 : « Imaginez que vous constatez un débit d'argent sur votre compte bancaire vous êtes certain de ne pas avoir réalisé vous-même. Vous pensez/ imaginez alors que votre numéro de carte de crédit a été volé et/ou piraté. Que faites-vous ? : pouvez-vous nous indiquer la probabilité que vous réalisiez chacune des actions suivantes, sur une échelle allant de 1 (« absolument pas probable ») à 7 (« très fortement probable ») ? »

Nous nous sommes appuyés pour cela sur les résultats d'une enquête portant sur les types de violations de données (Karunakaran et al., 2018), nous permettant de mieux appréhender le type de violations de données personnelles les plus fréquentes et leur compréhension par les utilisateurs.

Ensuite, nous nous sommes basés sur différents travaux pour imaginer une typologie de réponses, comme indiqué dans le Tableau 52 ci-dessous (les réponses pouvant légèrement varier entre les 2 scénarios).

La structure générale du questionnaire est présentée en Annexe 13. Le questionnaire a été généralement apprécié par les répondants (exemples de messages reçus de la part des répondants : « super sondage », « c'était vraiment très intéressant et j'ai trouvé que cela pousse à réfléchir sur nos comportements en ligne et tout ce que nous pouvons y mettre sans se douter que cela puisse être exploité par des personnes malveillantes », « juste j'ai beaucoup aimé ce questionnaire », « enquête très intéressante et plaisante à suivre »).

Tableau 52 : Typologie de réponses face à une violation de données personnelles

Item	Catégorie modèle	Références
Je ne fais rien	Pas d'action	Pas de référence
Je change mes codes d'accès au site Internet et met un mot de passe sécurisé	Action portant sur les données elles-mêmes ou actions techniques	Mamonov & Benbunan-Fish (2018)
Je contacte par téléphone ou e-mail le site Internet en question pour bloquer l'accès à mon compte en ligne		Son & Kim (2008), Smith et al. (1996)
J'en parle à mes proches	WOM ou e-WOM	Son & Kim (2008), Singh (1988), Lee & Cude (2012)
J'exprime mon mécontentement sur des réseaux sociaux ou sur des blogs		Lee & Cude (2012)
Je contacte par e-mail ou par téléphone le site Internet pour demander réparation	Plainte à l'entreprise, à l'autorité en charge de la protection des données personnelles ou à un tiers	Lee & Cude (2012)
Je contacte une association de protection des consommateurs ou un élu pour me défendre et obtenir réparation		Son & Kim (2008), Smith et al. (1996), Lee & Cude (2012)
Je porte plainte à la CNIL		-
Je demande le soutien d'une association ou d'un avocat pour lancer une action en justice afin d'obtenir réparation	Actions légales	Lee & Cude (2012)
Je vais porter plainte à la police		-

1.3. Variables de contrôle

Nous avons mesuré plusieurs variables de contrôle.

Premièrement, nous avons souhaité mesurer la tendance des individus à se plaindre dans le cas d'une insatisfaction. Nous ajoutons à cela une variable de contrôle pour évaluer cette tendance : « Que faites-vous lorsqu'un achat ne correspond pas avec ce qui vous était proposé (par exemple, erreur de livraison, promotion non prise en compte, chambre d'hôtel sale ou non conforme à l'annonce, problème dans une location de voitures ou lors d'une réservation de vacances, retard de train ou d'avion ...) ? ».

Deuxièmement, il nous est apparu important de contrôler l'expérience passée en termes de violations de données, qui peut influencer la perception et le comportement de réponse. Nous avons pris comme base de référence la liste des dommages potentiels de Karunakaran et al. (2018), à laquelle nous avons ajouté la question suivante : « Avez-vous déjà été victime d'une violation de vos données personnelles ? Si oui, laquelle ? et il y a combien de temps ? (Plusieurs réponses possibles) » (exemples de dommages : piratage du réseau de son entreprise, chantage à la webcam).

Troisièmement, nous avons souhaité mesurer l'effet de variables d'intentions comportementales : la *privacy self-efficacy*, i.e., l'évaluation que chacun fait de sa capacité à protéger sa vie privée en ligne (Mamonov & Benbunan-Fich, 2018) et les normes subjectives, i.e., les perceptions des individus de la pression sociale, représentée par ce que pensent les proches du comportement prévu ou entrepris (Ajzen, 1991). La *privacy self-efficacy* a été mesurée à l'aide des items extraits de Mamonov & Benbunan-Fich (2018). Les normes subjectives ont été mesurées à l'aide d'items extraits de Nguyen et al. (2017), qui avaient été utilisées dans le cas du changement climatique, et réappliquées à notre contexte de violation de données personnelles.

Enfin, nous avons inclus plusieurs questions sociodémographiques, dont l'âge. En effet, les préoccupations en matière de vie privée et pour la protection des données personnelles diffèrent selon l'âge (Hoofnagle et al., 2010; Jones et al., 2009; Miltgen & Peyrat-Guillard, 2014). De plus, les personnes d'une même génération (quelle qu'elle soit) partagent certaines valeurs culturelles et priorités communes (Jackson et al., 2011; Poeschel et al., 2020).

1.4. Échantillon

Le questionnaire a été administré en ligne auprès de 452 panélistes français, par l'institut professionnel d'études de marché PanelLabs. L'échantillon est équilibré en genre (53.3% d'hommes et 46.7% de femmes) et en termes d'activités professionnelles, la moyenne d'âge est de 44.8 ans (avec 46.5% des personnes interrogées qui ont entre 25 et 44 ans). Les détails des caractéristiques de l'échantillon sont fournis en Annexe 14. Les données ont été collectées entre le 9 et le 16/08/2021.

Les orientations culturelles individuelles peuvent varier entre les personnes d'un même pays (Oyserman et al., 2002). Il est alors intéressant d'interroger des personnes d'un même pays. De plus, le choix d'une administration du questionnaire uniquement en France est pertinent pour deux raisons :

- D'une part, la France fait partie des pays pionniers en Europe en matière de protection de la vie privée (la CNIL en France, et le Bundesbeauftragter für den Datenschutz und die Informationsfreiheit en Allemagne, ont été créés en janvier 1978, suivi en 1984 par l'Information Commissioner's Office au Royaume-Uni) ;
- D'autre part, la France est un pays sensible et médian au sein de l'Europe en termes d'appropriation du RGPD (e.g., en 3^{ème} position dans le classement des pénalités imposées par les autorités nationales, après le Luxembourg et l'Irlande ; en 9^{ème} position dans le classement du nombre de notifications de violations de données personnelles entre le 25 mai 2018 et le 27 janvier 2022, après l'Allemagne, les Pays Bas, le Royaume-Uni, la Pologne, le Danemark, l'Irlande, la Suède et la Finlande¹¹⁹).

¹¹⁹ DLA Piper GDPR fines and data breach survey. *op. cit.*

1.5. Ajustement des échelles

Nous avons appliqué une procédure classique d'épuration des dimensions par analyses factorielles successives. Malgré la consistance annoncée de certaines échelles, nous avons malheureusement constaté que plusieurs items ne permettaient pas d'aboutir à des résultats pertinents. Chaque orientation de l'échelle de Sharma a été réduite de 8 items initiaux à 3 ou 4 items (cf. Tableau 51).

Les items de mesure de la distance psychologique ont également été réduits comme suit :

- L'item de distance temporelle a été supprimé car il présentait très peu de variance. Ce point nous semble très intéressant car les recherches insistaient sur le rôle de la relation au temps dans les mécanismes cognitifs justifiant l'influence de la culture dans les représentations mentales d'événements futurs (Eyal et al., 2009). Nous reparlerons de ce point dans la discussion ;
- Après épuration, la distance psychologique est réduite à 3 items, un item pour chaque distance (sociale, spatiale et hypothétique). Nous avons été moins surpris par les ajustements à apporter à cette échelle, n'ayant pas de comparatif particulier car il n'existe pas d'échelle de mesure de la distance psychologique appliquée à la *privacy* (Bandara et al., 2021).

La totalité des items a été conservée pour le construit de préoccupation pour la protection des données personnelles ainsi que les réponses en termes techniques, sociales et institutionnelles. Les items de *privacy self-efficacy* et les normes subjectives convergent : ceci peut être dû au fait que les items sont présentés ensemble et vers la fin du questionnaire. Nous avons alors fait le choix de ne garder que la *privacy self-efficacy* afin d'en mesurer les effets complémentaires.

2. Résultats

2.1. Fréquences de violations de données

Presque deux tiers (62.2% ; N=281) des répondants ont déjà fait l'expérience d'une ou de plusieurs violations de données. Les violations liées à l'usage des outils informatiques sont premièrement les plus fréquentes avec (i) le piratage de messagerie et l'envoi de spams à partir du compte mail attaché (30.8% des cas) et (ii) le blocage de l'accès à son ordinateur et infection de l'ordinateur par un virus (29.4% des cas). Deuxièmement, 21.1% des répondants déclarent avoir subi un vol de numéro de carte bancaire suivi de retraits d'argent ou d'achats en ligne. Troisièmement, le piratage de compte Facebook et l'envoi de messages depuis ce compte représentent 17% des cas. Enfin dans une moindre mesure, les violations de données peuvent être liées au piratage du réseau d'entreprise (10.6%), au chantage à la webcam (8.4% des cas), à la prise en main du téléphone (6.4%), et à la demande de rançon (6.6%).

2.2. Méthodes d'équations structurelles, ajustement global du modèle et indices de validité

Les relations entre concepts sont mesurées grâce une modélisation pour équations structurelles, réalisée avec le logiciel XL-STAT/PLSPM.

Le modèle présente une qualité générale externe et interne satisfaite. Dans les deux scénarios de violations de données personnelles, les valeurs absolues de *goodness-of-fit* (Absolute GoF) sont satisfaisantes (0,306 pour le scénario 1 et 0,320 pour le scénario 2 ; cf. Tableau 51), selon les normes de Wetzels et al. (2009), et les statistiques de GoF basées sur les modèles internes et externes sont très élevées (supérieures à .85), confirmant la qualité globale du modèle.

Comme indiqué dans le Tableau 51, tous les *cross-loadings* sont supérieurs ou égaux à 0.5, confirmant la fiabilité des indicateurs. De plus, tous les standards de fiabilité (*reliability standards*) sont également satisfaits ($> 0,7$), selon Kapferer & Valette-Florence (2019), confirmant la cohérence interne du modèle. Enfin, les *Average Variance Extracted* (AVE) sont supérieurs au seuil minimum de 0.5 (Bagozzi and Yi, 1988). Nous obtenons une structure claire et bien délimitée de notre modèle.

2.3. Invariance des mesures

Avant de conduire une analyse multi-groupes avec test de permutation, nous devons d'abord vérifier que chaque sous-modèle considéré atteint bien une qualité d'ajustement acceptable et vérifier la condition d'invariance des mesures (Eberl, 2010). Comme le rappelle Chin et al. (2016), établir l'équivalence des mesures est essentiel pour les recherches, qui reposent sur des construits latents et des analyses multi-groupes. En effet, « sans équivalence des mesures, les conclusions basées sur les échelles de mesure, telles que la signification et l'interprétation des construits latents ou la détermination des différences ou des équivalences entre les populations, peuvent au mieux être ambiguës, ou pire, invalides » (Chin et al., 2016, p.1).

Pour nous assurer de l'équivalence des échelles de réponses entre les deux échantillons correspondant à nos deux scénarios, nous avons donc procédé à un test d'invariance multi-groupes dont les résultats sont présentés ci-dessous :

Tableau 53 : Mesure des corrélations des mesures entre les scénario 1 et 2

Variable latente	Variables manifestes	Différence	P	Significatif
Réponses techniques	Rép. Technique 1	0,458	0,000	Oui
	Rép. Technique 2	0,061	0,052	Non
	Rép. Technique 3	0,070	0,001	Oui
Réponses sociales	Rép. Sociale 1	0,060	0,210	Non
	Rép. Sociale 2	0,113	0,024	Oui
Réponses institutionnelles	Rép. Inst. 1	0,003	0,884	Non
	Rép. Inst. 2	0,008	0,716	Non
	Rép. Inst. 3	0,000	0,995	Non
	Rép. Inst. 4	0,123	0,000	Oui

De fait, au seuil de 5%, et avec 5000 permutations, 4 items sur 9 montrent de la variance entre le scénario 1 et le scénario 2. Nous évaluons donc l'importance de cette différence en calculant, pour chaque échelle, la variance dans la mesure liée à la différence de scénario et obtenons 0.07 pour les réponses privées, 0.005 pour les réponses sociales et 0.004 pour les réponses publiques. Nous en déduisons un impact négligeable du scénario sur la variance dans la mesure et procédons donc à l'interprétation des résultats par scénario.

2.4. Tests des hypothèses

Les résultats sont présentés dans les Tableau 54 et Tableau 55 ainsi que les Figure 40 et Figure 41. Ils montrent que 12 de nos 17 hypothèses initiales sont corroborées dans les deux scénarios. H1, H2b, H4a et H6a ne sont corroborées dans aucun des deux scénarios. H7a n'est corroborée que dans le scénario 2 (i.e., piratage de carte de crédit).

Premièrement, notre recherche prouve que l'ajout de la distance psychologique avec la violation de données personnelles est justifié car la modélisation montre que ce construit agit significativement et que son pouvoir explicatif dans les mécanismes observés est supérieur à celui de la préoccupation pour la protection des données personnelles.

Deuxièmement, les orientations culturelles les plus importantes influençant à la fois les préoccupations en matière de protection des données personnelles et la distance psychologique avec la violation de données sont l'inégalité sociale et l'égalité des genres. Une orientation vers l'indépendance influence positivement les préoccupations pour la protection des données personnelles (0,18) mais n'affecte pas la distance psychologique avec la violation de données ($p = 0,9$). Une préférence pour les valeurs traditionnelles ou une aversion au risque ont des effets mineurs. En effet, une préférence pour les valeurs traditionnelles influence positivement la distance psychologique avec la violation de données personnelles (0,12) mais n'a pas d'impact sur la préoccupation pour la protection des données ($p > 0,3$), soulignant qu'il n'y a pas de relation entre la préoccupation concernant la confidentialité et les valeurs traditionnelles de moralité. Ainsi nos hypothèses H2b, H4a et H6a ne sont pas corroborées.

Troisièmement, la préoccupation pour la protection des données personnelles et la distance psychologique avec la violation de données personnelles influencent tous les types de réponses, mais c'est à cette étape du modèle qu'apparaissent des différences entre les deux scénarios. D'une part, la distance psychologique influence négativement les réponses techniques, mais l'effet significatif dans le scénario 2 ($p < .01$) ne se retrouve pas dans le scénario 1. D'autre part, la distance psychologique et la préoccupation pour la protection des données personnelles activent des réponses sociales face à une violation de données personnelles mais à des degrés différents. Cela doit s'expliquer par le fait que dans le cas d'un vol de données bancaires, les gens en parlent à leurs proches, alors que dans le cas d'une fuite de données d'un réseau social ou d'un site marchand, les gens partagent cette expérience sur les réseaux sociaux.

Enfin, la relation entre la distance psychologique avec la violation de données personnelles et la préoccupation pour la protection des données personnelles n'est pas significative ($R^2 = 0.01$; $p > .5$; H1 rejetée).

2.5. Variables de contrôle

L'âge n'influence ni la distance psychologique avec la violation de données personnelles ni la préoccupation pour la protection des données personnelles de façon significative pour les deux scénarios ($R^2 < .06$; $p > .05$). La *privacy self-efficacy* et la tendance à se plaindre influencent significativement les réponses techniques pour les deux scénarios ($R^2 > 0.17$; $p < .1$). Les effets ne sont pas significatifs pour les réponses sociales et institutionnelles : le sentiment d'être en capacité de protéger sa vie privée (*self-efficacy*) ou la tendance à se plaindre lors d'un achat insatisfait est corrélé avec l'activation de moyens techniques pour se protéger. Ceci est cohérent avec les résultats de Bandara et al. (2021) qui montrent que le sentiment d'*empowerment* diminue l'effet de la distance psychologique sur les comportements défensifs.

Tableau 54 : Résultats pour le scénario 1 (cas de piratage de ses accès à un site Internet)**Structural path coefficient estimates**

Results for scenario 1				
Latent predictors	Parameter estimates	Pr > t	Low confidence intervals (95%)	High confidence intervals (95%)
Dependent variable: Information Privacy Concern; $R^2 = 0.155$				
Independence	0,187	0,000	0,074	0,306
Risk aversion	0,090	0,062	-0,023	0,204
Social inequality	-0,204	0,000	-0,332	-0,087
Gender Equality	0,172	0,001	0,041	0,298
Tradition oriented	0,041	0,372	-0,072	0,140
Psychological distance with Data Breaches	0,016	0,753	-0,111	0,204
Dependent variable: Psychological distance with Data Breaches; $R^2 = 0.260$				
Independence	-0,004	0,924	-0,142	0,070
Risk aversion	-0,102	0,023	-0,238	0,025
Social inequality	0,370	0,000	0,215	0,468
Gender Equality	-0,254	0,000	-0,348	-0,147
Tradition oriented	0,123	0,004	-0,015	0,201
Dependent variable: Technical privacy protective responses; $R^2 = 0.155$				
Psychological distance with Data Breaches	-0,067	0,164	-0,174	0,122
Information Privacy Concern	0,233	0,000	0,130	0,362
Dependent variable: Social privacy protective responses; $R^2 = 0.066$				
Psychological distance with Data Breaches	0,102	0,043	-0,098	0,256
Information Privacy Concern	0,230	0,000	0,110	0,336
Dependent variable: Institutionnal privacy protective responses; $R^2 = 0.095$				
Psychological distance with Data Breaches	0,234	0,000	0,128	0,347
Information Privacy Concern	0,186	0,000	0,099	0,302

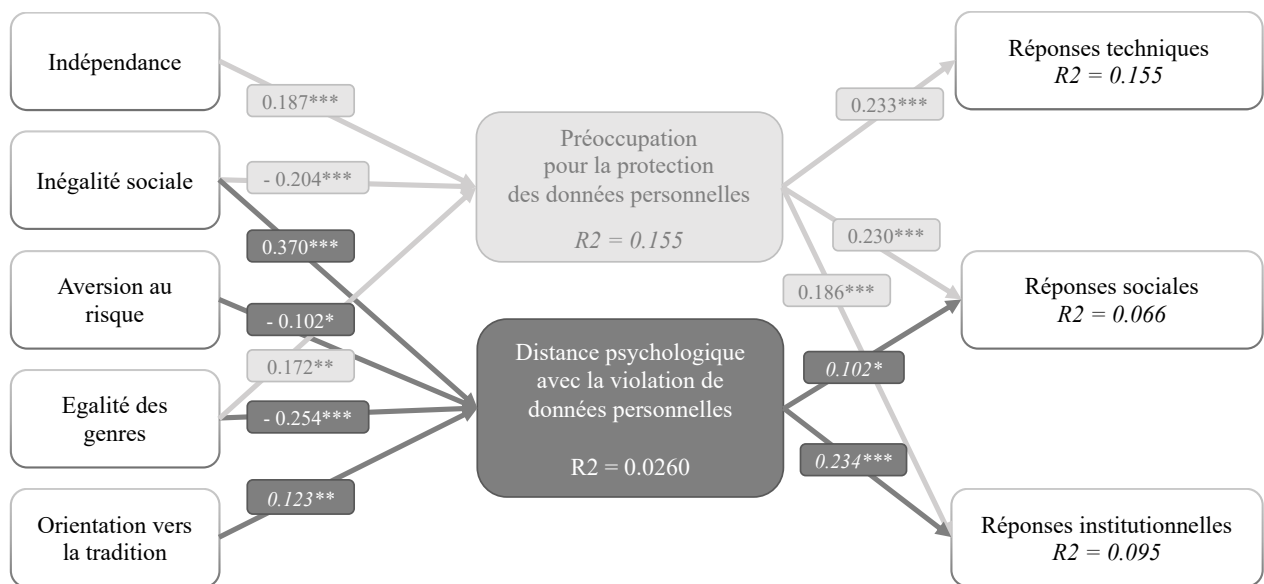
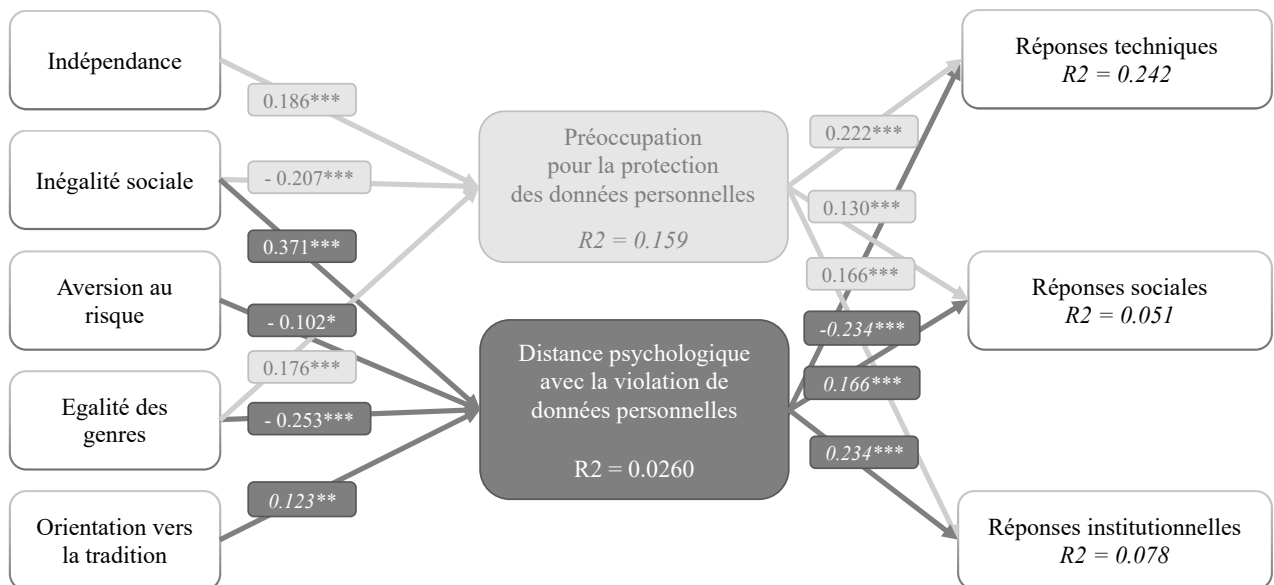
In bold: $p < .05$ **Figure 40 : Résultats obtenus avec le scénario 1**** $p < .05$, ** $p < .01$, *** $p < .001$*

Tableau 55 : Résultats pour le scénario 2 (cas de piratage de sa carte de crédit bancaire)**Structural path coefficient estimates**

Results for scenario 2				
Latent predictors	Parameter estimates	Pr > t	Low confidence intervals (95%)	High confidence intervals (95%)
Dependent variable: Information Privacy Concern; $R^2 = 0.159$				
Independence	0,186	0,000	0,094	0,277
Risk aversion	0,090	0,060	-0,063	0,230
Social inequality	-0,207	0,000	-0,340	-0,066
Gender Equality	0,176	0,000	0,045	0,297
Tradition oriented	0,042	0,358	-0,076	0,143
Psychological distance with Data Breaches	0,011	0,834	-0,134	0,155
Dependent variable: Psychological distance with Data Breaches; $R^2 = 0.260$				
Independence	-0,005	0,916	-0,091	0,099
Risk aversion	-0,102	0,022	-0,226	0,059
Social inequality	0,371	0,000	0,255	0,497
Gender Equality	-0,253	0,000	-0,360	-0,156
Tradition oriented	0,123	0,004	-0,042	0,216
Dependent variable: Technical privacy protective responses; $R^2 = 0.242$				
Psychological distance with Data Breaches	-0,234	0,000	-0,372	-0,101
Information Privacy Concern	0,222	0,000	0,094	0,343
Dependent variable: Social privacy protective responses; $R^2 = 0.051$				
Psychological distance with Data Breaches	0,166	0,001	-0,142	0,275
Information Privacy Concern	0,130	0,007	0,012	0,367
Dependent variable: Institutionnal privacy protective responses; $R^2 = 0.078$				
Psychological distance with Data Breaches	0,234	0,000	0,114	0,318
Information Privacy Concern	0,166	0,000	0,052	0,285

In bold: $p < .05$ **Figure 41 : Résultats pour le scénario 2*** $p < .05$, ** $p < .01$, *** $p < .001$

Section 4. Discussion et implications

Cette recherche vise à comprendre l'influence des orientations culturelles individuelles sur le comportement de réponses face à une violation de données personnelles, ainsi que les mécanismes psychologiques reliant orientation culturelle et réponses. Cette recherche a mis en lumière des résultats importants permettant de répondre à cet objectif. Plusieurs points sont développés et approfondis dans le chapitre 7 du manuscrit (discussion).

Premièrement, l'orientation culturelle qui influe le plus sur les mécanismes psychologiques de réponses est l'**égalité socio-genrée** (égalité des genres et inégalité sociale). L'indépendance n'affecte que peu la préoccupation, et ne rend pas la violation de données personnelles plus concrète. L'aversion au risque joue un rôle mineur, tandis que l'orientation traditionnelle n'affecte que la préoccupation psychologique. Ces résultats sont concordants avec ceux de Milberg et al. (2000) qui montrent que les dimensions d'Hofstede qui ont le poids le plus important sont la distance hiérarchique (.77), la masculinité (.56), le contrôle de l'incertitude (-.37) et l'individualisme (.31) : notre recherche remet en lumière ce constat et apporte des contributions théoriques importantes sur ce sujet, que nous détaillons dans le prochain paragraphe.

D'autre part, cette recherche apporte des **éléments de réflexion sur les réponses apportées par les consommateurs face à une violation de leurs données personnelles**, montrant notamment que plus les violations de données personnelles sont concrètes, plus les réponses sont techniques et individuelles ; ou bien également qu'une tendance à se plaindre dans le cas d'un achat insatisfait va surtout se transformer en action technique dans le cas d'une violation de données personnelles.

Enfin, cette recherche met en lumière les mécanismes psychologiques dans les réponses de protection de la vie privée et montre le **rôle important de la distance psychologique avec la violation de données personnelles dans ces mécanismes**. Ainsi alors que les réponses des consommateurs face à une violation de leurs données personnelles restent un champ encore sous-exploité (Labrecque, 2021), malgré l'importance croissante de ces phénomènes ; et alors que le rôle de la distance psychologique dans les réactions pour la protection de sa vie privée vient très récemment d'être mis en lumière (Bandara et al., 2021), alors que ce construit a montré son efficacité dans le cas du changement climatique (Singh et al., 2017), notre recherche apporte des contributions tant théoriques que managériales.

1. Contributions théoriques

Tout d'abord, cette recherche contribue à combler une lacune dans la **compréhension des liens entre la culture et la vie privée**. D'une part, elle répond à un appel important d'utiliser un modèle autre que celui de la culture nationale d'Hofstede (e.g., Miltgen & Peyrat-Guillard, 2014). D'autre part, elle permet de sortir d'un dialogue « sans fin » dans la compréhension des liens entre une préférence pour des valeurs culturelles d'individualisme ou d'indépendance et la préoccupation pour la protection des données personnelles (Martin & Murphy, 2017). Notre recherche élargit en effet le spectre des dimensions qui sont étudiées, les évalue à un niveau individuel et minore l'importance accordée à l'individualisme dans son lien avec la préoccupation pour la protection de la vie privée.

Deuxièmement, cette recherche **complète les travaux récents sur le concept de distance psychologique avec la vie privée** (Bandara et al., 2021), en traitant de la distance psychologique avec la violation de données personnelles. De plus, nos résultats interrogent le rôle de la distance temporelle, qui semble ne pas être significatif, contrairement au cas du changement climatique et aux hypothèses de Bandara et al. (2021). Enfin, elle avance des éléments permettant par la suite de définir une échelle de mesure de la distance psychologique avec la violation de données personnelles.

Troisièmement, cette recherche **rafraîchit la taxonomie des réponses de protection de la vie privée** (Son & Kim, 2008). Elle identifie également des éléments qui pourraient enrichir le champ de la *consumer complaint behaviour*, en élargissant au cas des violations de données personnelles. Nous démontrons que les mécanismes de réponse pourraient ne pas être les mêmes dans le cas des violations de données : alors qu'Internet augmente les possibilités de prise de parole des consommateurs insatisfaits, les réponses pourraient être de plus en plus techniques dans le cas des violations de la vie privée. De plus, nos résultats semblent valider le fait que le sentiment d'être en capacité de protéger sa vie privée ou la tendance à se plaindre lors d'un achat insatisfait sont corrélés avec l'activation de moyens techniques pour se protéger.

2. Implications pratiques

En éclairant les mécanismes psychologiques reliant orientations culturelles et réponses du consommateur face à une violation de données personnelles, en identifiant des valeurs significatives et de nouveaux types de réponses, notre recherche identifie des leviers d’actions pour les politiques publiques et les entreprises, soucieuses de protéger la vie privée de chacun(e) quelles que soient ses préférences culturelles partagées dans un groupe social. Nous les indiquons ci-dessous et nous renvoyons le lecteur en particulier vers le chapitre 7 pour compléter les implications pratiques et managériales de cette recherche.

2.1. Vers des actions adaptées aux groupes sociaux et à leurs préférences en termes de valeurs culturelles

En montrant que la distance psychologique avec la violation de données personnelles joue un rôle de premier ordre dans la réponse du consommateur face à une violation de données personnelles et que l’égalité socio-genrée est l’orientation culturelle la plus influente, cette recherche fait écho aux travaux de Pasquier (2018) sur l’Internet des familles rurales. Nous mettons en avant le fait que les familles modestes se soucient essentiellement du piratage et de l’usurpation d’identité, mais pas du tout de la protection des données personnelles ou de la souveraineté numérique, et que la conception de la vie privée relève moins de l’individu que du groupe familial. Ces résultats permettent à la CNIL d’éclairer un rapport alternatif aux technologies et à la protection des données personnelles, qui vient enrichir les pistes d’actions des services publics, notamment pour répondre à une exigence de fracture numérique et d’impératif de désenclavement face au tout numérique des services publics.

2.2. Vers un exercice du droit plus collectif

Ce constat d’importance de l’égalité socio-genrée répond également aux appels de plusieurs chercheurs, selon lesquels « il paraît nécessaire de cesser de penser individuellement la vie privée, de cesser de la considérer comme un arbitrage que chacun serait amené à faire. Nous devons plutôt y réfléchir comme un droit collectif, par lequel, même si nous n’avons rien à cacher, il est aussi dans l’intérêt de tous de vivre dans une société où certains (...) puissent avoir

des choses à cacher » (Cardon, 2019, p.418). Si la protection des données personnelles est un droit privé, les leviers d'action qui la concernent sont de nature collective.

Alors que nos réglementations se basent sur un droit individuel et une responsabilité personnelle de protection de sa vie privée, il serait intéressant d'interroger les valeurs et les normes qui sous-tendent nos réglementations, et peut-être de revoir ces dernières (Solove, 2020).

2.3. Vers des actions de communication plus adaptées

Par ailleurs, cette recherche identifie plusieurs leviers d'action marketing qui peuvent être activés par des acteurs publics ou privés dans un objectif de sensibilisation des populations et de changement des comportements, à travers notamment des actions de communication. D'une part en mobilisant les leviers du marketing social, selon les objectifs (e.g., renforcer les actions techniques individuelles pour protéger les données personnelles, amener les individus à se plaindre davantage afin d'identifier plus facilement les problèmes de violation de données) et les orientations culturelles des populations ciblées. D'autre part, en activant différents niveaux de distance psychologique, et en jouant sur les niveaux de représentation et d'abstraction aboutissant à des évaluations des risques positifs ou négatifs. Par exemple, une représentation abstraite telle que « protéger sa vie privée » pourrait conduire à une évaluation plus positive de cette activité alors qu'une représentation concrète comme « arrêter d'utiliser WhatsApp » ou « n'accepter aucun cookie sur les pages web » pourrait aboutir à une évaluation négative de cette même activité.

Enfin, nos résultats, obtenus dans le cadre hexagonal, permettent de comprendre la variabilité au niveau international dans le nombre de plaintes notifiées pour violations de données personnelles, notamment entre pays européens¹²⁰, mais également en incluant les pays en développement et les BRICS, pays quasi ignorés par la recherche sur les données personnelles malgré les échanges internationaux de données et les principes d'extraterritorialité de nos réglementations (e.g., application du RGPD dans les pays du Maghreb pour l'offshoring de services).

¹²⁰ DLA Piper GDPR fines and data breach survey. *op. cit.*

3. Limites et voies de recherche

Bien entendu, notre recherche comporte des limites qui ouvrent la voie à de futures recherches.

En premier lieu, certaines questions concernant principalement les contextes et les types de violation de données personnelles demeurent. Par exemple, nous avons testé deux scénarios de violations de données : piratage de l'accès à un site Internet et piratage d'une carte de crédit. De nouveaux tests avec d'autres scénarios de violation, au regard du fait que près de deux tiers de nos répondants ont déjà été victime d'une violation de données, principalement liées à l'usage des outils informatiques, apporteraient plus de matière au sujet.

En second lieu, il serait intéressant de mieux comprendre les effets d'une vision de soi « interdépendante ». L'indépendance et l'interdépendance représentent différentes manières d'envisager la construction de soi et ne sont pas corrélées négativement. L'indépendance représente une préférence pour une construction de soi autonome et individuelle alors que l'interdépendance représente une préférence pour une construction de soi au sein d'un groupe social. Nos résultats ne portent que sur l'indépendance. Il serait pertinent d'éclairer le lien entre interdépendance et comportement de réponses face à une violation de données personnelles. Dans cette perspective, notre recherche conduite sur l'influence des normes socio culturelles à un niveau méso pourra offrir de premières réponses.

Troisièmement, une exploration en profondeur des différentes dimensions de la distance psychologique s'impose, à la fois dans le lien entre orientations culturelles et dimensions de la distance psychologique (e.g., lien entre distance sociale et relation à l'*endogroupe* et à l'*exogroupe*) que dans le lien entre dimensions de la distance psychologique et types de réponses (e.g., quel impact de la distance hypothétique sur les différents types de réponses ?). Ceci permettrait notamment de mieux comprendre le rôle de la culture dans les représentations mentales (Shapira et al. 2012), alors que trop peu d'études s'intéressent à l'influence des variations culturelles dans les processus cognitifs (Wiesenfeld et al., 2017).

Synthèse de l'essai 3

Notre dernier essai n°3 a pour objectif d'étudier à un niveau micro l'influence des orientations culturelles individuelles sur le comportement de réponse face à une violation de données personnelles, ainsi que les mécanismes psychologiques reliant orientations culturelles et réponses.

Cette recherche confirme d'une part l'importance d'une préférence culturelle pour l'égalité socio-genrée, et met d'autre part en lumière le rôle prépondérant de la distance psychologique, par rapport à la préoccupation pour la protection de ses données personnelles.

Cette recherche porte de nombreuses contributions théoriques prometteuses. Les résultats obtenus viennent également enrichir notre thèse dont nous sommes maintenant heureux de pouvoir discuter des résultats dans leur globalité dans le chapitre suivant.

Chapitre 1. Contexte général de la thèse



Chapitre 2. Fondements théoriques

Protection
des données
personnelles

Réponses des
consommateurs
insatisfaits

Culture
et valeurs



Chapitre 3. Cadre général de la thèse



Réponses à une violation de données personnelles :
3 niveaux d'observation de l'influence de la culture

Chapitre 4.

Essai 1
Niveau
Macro :
Influence de
la culture
nationale

Chapitre 5.

Essai 2
Niveau
Meso :
Influence des
normes
socio-
culturelles

Chapitre 6.

Essai 3
Niveau
Micro :
Influence des
orientations
culturelles
individuelles



Chapitre 7. Discussion et conclusion

Chapitre 7. Discussion et conclusion



Ce dernier chapitre est l'aboutissement de notre thèse de doctorat. Après avoir repris les résultats de nos recherches, nous discutons leurs apports théoriques au regard des travaux actuels menés en vie privée (dans la section 1), exposons les implications pratiques qui peuvent être imaginées à partir de ces résultats (section 2), et enfin montrons les limites qui sont autant de voies de recherche à mettre à notre agenda de future chercheure (section 3).

Notre recherche distingue trois principaux résultats (répondant à nos trois questions de recherche initiales ; cf. page 78) : (i) la définition d'une typologie de réponses apportées face aux violations de données personnelles, (ii) l'identification de nouveaux effets culturels et d'une préférence pour des valeurs d'égalité sociale et de genre, (ii) l'identification de la protection de la vie privée comme une pratique sociale, reposant notamment sur une réduction de la distance psychologique avec les violations de données personnelles. Les résultats sont repris dans le Tableau 56 page suivante.

À partir de ces résultats, notre travail apporte plusieurs contributions significatives aux recherches en vie privée répondant à des interrogations en cours sur le lien entre culture et vie privée, et aussi sur les réponses des consommateurs en situation de vulnérabilité informatique (notamment face à des violations de données personnelles). Ceci nous amène à discuter une nouvelle compréhension de la préoccupation pour la protection de la vie privée, que nous proposons de définir comme **un souci de sécuriser les données personnelles de tous**.

Ces éléments théoriques sont la base de contributions pratiques, qui s'inscrivent dans un cadre général de développement de pratiques de protection de la vie privée à un niveau méso, autour des notions de **responsabilité et sécurité**. Nous abordons plusieurs propositions d'actions à destination des différents acteurs (e.g., entreprises, structures éducatives, collectivités), suggérons des initiatives en termes de communications publicitaires et médiatiques, et discutons des modifications à apporter aux réglementations.

Tableau 56 : Principaux résultats de chaque essai

	Essai 1 : Macro	Essai 2 : Méso	Essai 3 : Micro
	Influence de la culture nationale	Influence des normes socio-culturelles	Influence des orientations culturelles individuelles
Principaux résultats	- Mise en évidence d'un comportement spécifique : la plainte au régulateur - Influence positive de la féminité, de l'individualisme et de la tradition sur le comportement de plainte face à une violation de ses données personnelles - La préférence pour la féminité (souci de la communauté) et à la tradition sont plus importantes que la préférence pour l'individualisme	- Approfondissement de la typologie des différentes réponses face aux violations de données personnelles - Mise en évidence de la défense d'une égalité sociale comme une motivation essentielle à l'adoption d'une réponse active face aux violations de données personnelles - Les personnes peuvent aussi agir pour un idéal de liberté ou une volonté de sécurité - Identification de la question de la protection de la vie privée comme une pratique sociale	- Influence plus significative de l'égalité sociale et de l'égalité entre les genres sur les réponses, que de l'indépendance - L'aversion au risque et la préférence pour la tradition jouent un rôle mineur - Rôle essentiel de la distance psychologique avec les violations de données personnelles, qui minore l'importance de la préoccupation pour la protection de ses données personnelles - L'égalité socio-genrée implique moins de distance psychologique avec la violation de données et favorise des réponses techniques - L'indépendance n'encourage que la préoccupation pour la protection des données personnelles

Section 1. Contributions théoriques

À partir de nos résultats, notre travail apporte plusieurs contributions théoriques significatives aux recherches en vie privée, que nous discutons dans cette section (donnant ensuite lieu à des implications pratiques ; présentées dans la Figure 42 page suivante). Ces contributions théoriques sont les suivantes :

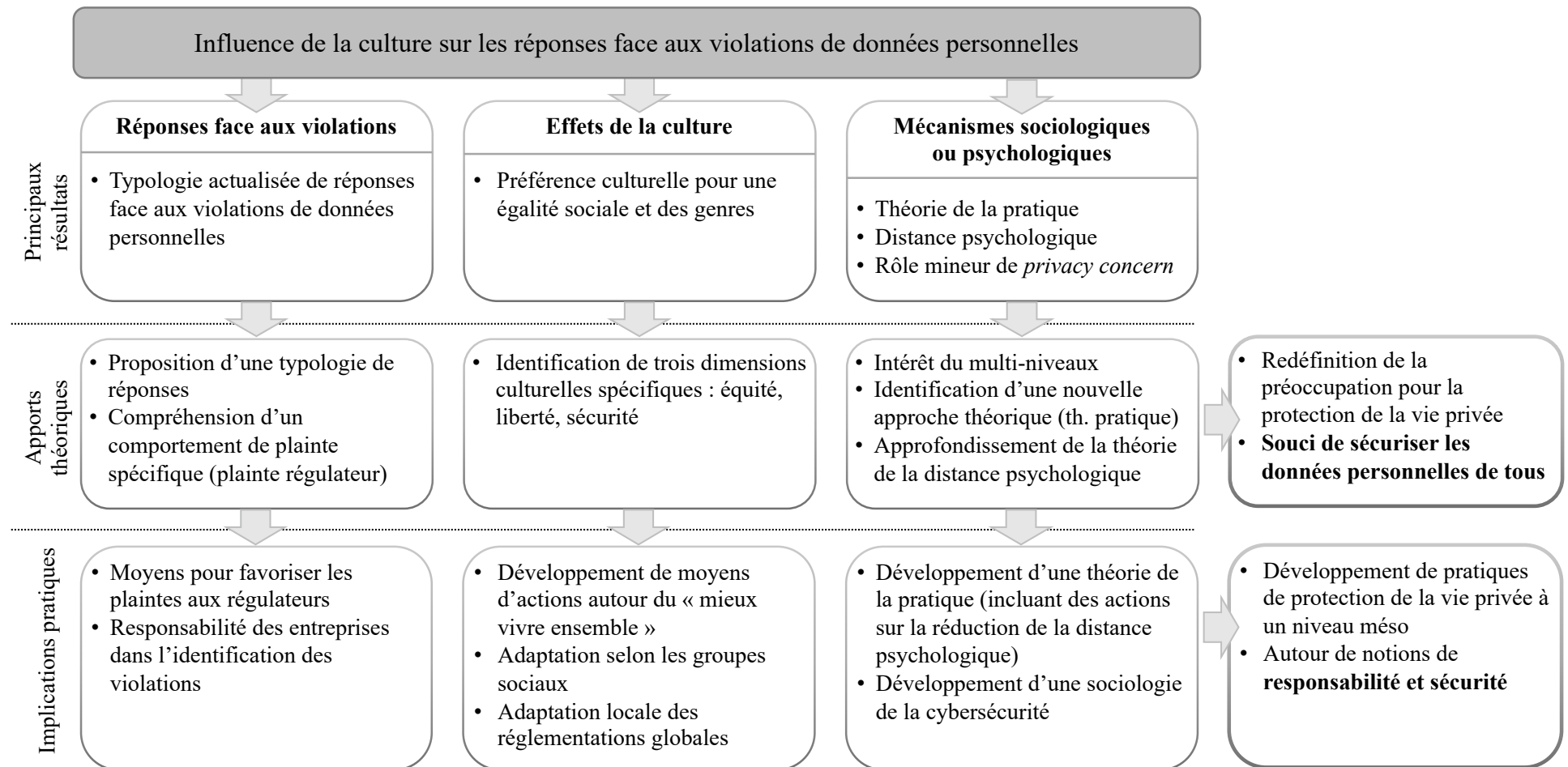
- (i) une compréhension différente des phénomènes et effets reliant culture et protection de la vie privée informationnelle, avec la prépondérance d'un souci d'équité sociale,
- (ii) un éclairage des réponses du consommateur dans une situation de vulnérabilité informatique et donc du lien entre vie privée et sécurité,
- (iii) un enrichissement des recherches sur la distance psychologique avec la vie privée, montrant son importance dans les réponses face à une violation,
- (iv) l'apport d'un nouveau cadre théorique à travers la théorie de la pratique, qui, nous l'espérons très sincèrement, ouvrira la voie à de nombreuses autres recherches,
- Et enfin (v) la possibilité d'une nouvelle compréhension de la préoccupation pour la protection de la vie privée informationnelle (*information privacy concern*).

En effet, ce sont les différents éclairages théoriques (équité sociale, lien entre vie privée et sécurité, importance de la distance psychologique, et pratique d'une protection de la vie privée) qui nous permettent d'enrichir notre compréhension de l'*information privacy concern*. **Ainsi être soucieux de la protection de sa vie privée, ce n'est pas vouloir contrôler ses propres données personnelles, c'est vouloir sécuriser les données personnelles de tous.**

Par là même, nos travaux remettent en question l'importance de l'individualisme comme valeur fondatrice de la protection des données personnelles, ainsi que l'importance accordée au souci de contrôle de ses données personnelles dans les mécanismes de réponses. Ils permettent également d'accorder plus d'importance à l'utilisateur-consommateur dans les situations de violations de données personnelles. Enfin nous avons la volonté d'ouvrir un champ entre vie privée et sécurité et d'intégrer les questions de cybersécurité dans la recherche en marketing.

Dans cette section, nous discutons la compréhension théorique des effets culturels (1), et des réponses aux violations de données personnelles (2), les apports aux recherches portant sur la distance psychologique avec la vie privée (3), l'identification de la théorie de la pratique comme un cadre de compréhension pour le développement de pratiques de protection de la vie privée (4), et enfin une nouvelle compréhension de la protection de la vie privée (5).

Figure 42 : Apports théoriques et pratiques des résultats de la recherche



1. Effets culturels sur les réponses aux violations de données personnelles

Notre recherche présente une quadruple originalité. Premièrement, elle mobilise une approche qualitative, alors que toutes les recherches identifiées (cf. pages 62 à 76) abordent la question de l'influence de la culture sur le souci de protection de la vie privée par une approche quantitative, à l'exception de la recherche d'Altman (1977). Ceci peut être dû au fait que les recherches sont essentiellement menées en systèmes d'information avec une posture positiviste, et confirme la nécessité d'intégrer une approche sociologique dans les recherches en sécurité informatique. Deuxièmement, nous utilisons une nouvelle échelle (Sharma, 2010) pour mesurer les effets culturels à un niveau individuel alors que la majorité des recherches s'appuient sur les dimensions de la culture nationale d'Hofstede (1984, 2001, 2010) (e.g., Liu & Wang, 2018; Trepte et al., 2017), opérant parfois une confusion entre niveaux macro et micro. Troisièmement, nous observons les effets culturels à un niveau méso, ce qui n'a jamais été fait à notre connaissance. Et quatrièmement, nous testons toutes les valeurs, offrant l'opportunité d'en comparer les effets relatifs.

Ainsi, nos travaux permettent d'identifier une nouvelle valeur prépondérante (que nous expliquons page suivante) : le souci d'équité sociale et de genre. Ils permettent de modérer l'importance de l'individualisme.

Nous reprenons ces informations dans le Tableau 57 ci-dessous et nous les discutons ensuite.

Tableau 57 : Principales valeurs culturelles identifiées

Essai	Méthodologie	Référentiel de valeurs	Valeurs culturelles identifiées (par ordre d'importance dans les effets)
Macro	- Quantitative	- Hofstede (1984, 2001, 2010)	- Féminité - Tradition - Individualisme
Méso	- Qualitative	- Aucune	- Équité sociale - Liberté - Sécurité
Micro	- Quantitative	- Sharma (2010)	- Inégalité sociale - Égalité de genre - Indépendance - Aversion au risque

1.1. Préférence culturelle pour des valeurs d'équité sociale et de genre

Dans notre thèse, nous défendons qu'une préférence culturelle pour des valeurs d'égalité sociale et de genre amène les individus à être plus engagés et actifs face à des violations de leurs données personnelles. Nous définissons la préférence culturelle pour des valeurs d'égalité sociale et de genre comme le désir que chaque individu puisse disposer des mêmes droits, opportunités et possibilités d'être protégés numériquement, indépendamment des différences sociales, de sexe, d'origine ou de la vulnérabilité. Chaque essai contribue à ce constat.

Le premier essai révèle qu'une préférence culturelle pour la féminité (e.g., les soins apportés aux autres) influence plus le comportement de plainte face à une violation de données personnelles (car les personnes portent plainte dans un souci de protection de leur entourage), qu'une préférence pour la tradition (les règles héritées et les plaintes étant privilégiées pour régler un problème) ou qu'une préférence pour l'individualisme (où la protection de la vie privée est légitime et de la responsabilité de chacun). À notre connaissance, seules les recherches de Milberg et al. (2000) et Bellman et al. (2004) identifient un effet de la « masculinité-féminité » sur la préoccupation pour la protection de la vie privée mais dans une direction opposée. Quelques recherches avaient mobilisé la dimension de « masculinité-féminité » (Cho et al., 2009 ; Li et al., 2017 ; Lowry et al., 2011) mais sans trouver d'effet particulier. Il existait donc une incompréhension des phénomènes. Nos deux autres recherches, méso et micro, confirment ces résultats :

- Le deuxième essai montre que la défense d'une équité sociale est une motivation essentielle à l'adoption de réponses actives face aux violations de données personnelles. Celles-ci sont techniques (pour rendre les moyens de protection actifs et accessibles), institutionnelles (e.g., plaintes collectives) ou sociales (e.g., soutien et formation). Les personnes peuvent également agir en poursuivant un idéal de liberté ou une volonté de sécurité ;
- Le troisième essai expose que l'égalité sociale et l'égalité entre les genres influencent le plus les mécanismes psychologiques de réponse. L'indépendance n'affecte que peu la préoccupation, et ne rend pas la violation de données personnelles plus concrète. L'aversion au risque joue un rôle mineur, tandis que l'orientation traditionnelle n'affecte que la préoccupation psychologique.

Notre recherche apporte clairement une nouvelle compréhension des effets culturels sur les réponses pour la protection de la vie privée : il s'agit de l'apport majeur de notre thèse.

1.2. Compréhension d'une préférence culturelle pour l'individualité autour de deux axes : liberté et sécurité

En dehors de ce constat majeur, plusieurs préférences culturelles ont un effet : tradition et individualisme (macro), liberté et sécurité (méso), indépendance et aversion au risque (micro). Dans notre essai micro, l'aversion au risque joue un rôle mineur, tandis que l'orientation traditionnelle n'affecte que la préoccupation psychologique. Pour cette raison, nous isolons dans notre réflexion trois préférences culturelles : l'individualisme, l'indépendance et la sécurité.

Nous soutenons que l'individualisme (pour lequel la protection de la vie privée est légitime et de la responsabilité de chacun) et l'indépendance sont l'expression de 2 préférences :

- la liberté (également nommé *self-direction* ; Kaasa, 2021). Par exemple à un niveau micro, l'indépendance est majoritairement comprise comme la liberté individuelle (i.e. « je compte sur moi-même » ; cf. Tableau 51 p. 231),
- la sécurité individuelle (*affective autonomy* ; Schwartz, 2006). En effet à un niveau méso, l'individualité déclarée (e.g., « protéger sa tranquillité et son jardin secret ») est en définitive l'expression d'un « imaginaire de sécurité » qui consiste à protéger son intimité et la sécurité familiale.

En conclusion, notre recherche identifie l'importance de trois valeurs culturelles : équité sociale, liberté, sécurité.

2. Réponses aux violations de données personnelles

Le second apport théorique de notre recherche réside dans l'exploration des réponses de protection de données personnelles, et en particulier face aux violations de données personnelles. Pour cela, nous proposons une typologie de réponses (2.1.), et parmi celles-ci, nous identifions un comportement particulier : la plainte au régulateur (2.2.).

2.1. Proposition d'une typologie de réponses de protection de la vie privée

Comme nous l'avons indiqué dans notre revue de la littérature (pages 121 à 125), Son & Kim (2008) ont proposé une taxonomie de réponses pour la protection des données personnelles (*privacy protective responses*). Depuis 2008, de nouvelles possibilités de réponses ont été explorées : mesures de sécurité, authentification, contrôle d'accès (Labrecque, 2021; Mamonov & Benbunan-Fich, 2018), non-divulgaration ou falsification d'informations (Miltgen & Smith, 2019), actions en justice (Mamonov & Benbunan-Fich, 2018; Romanosky et al., 2013). Quach et al. (2022) proposent une classification des comportements des consommateurs de protection de données personnelles : mais cette classification se limite à certains types de réponses (e.g., réactives, comme la falsification, ou proactives, comme la restriction d'informations), et n'intègre pas toutes les possibilités qui s'offrent à un individu face à une violation de ses données personnelles.

Notre recherche répond clairement à cet objectif en distinguant des réponses techniques, sociales et institutionnelles. Cette classification a été éprouvée dans deux essais (méso et micro) et a été bien comprise par les répondants, ce qui nous a également permis d'actualiser les réponses, d'en reclassifier certaines et d'identifier les limites de quelques possibilités. Nous proposons donc une typologie agrégée et actualisée, en prolongement de celle de Son & Kim (2008).

De plus, notre typologie est centrée sur les réponses des individus-consommateurs en vue de les aider et de les dédommager. Les précédentes recherches (e.g., Quach et al., 2022) mettent les réponses des consommateurs au regard des réponses des entreprises et des régulateurs, afin d'offrir une vision globale des possibilités d'atténuer les risques d'atteinte à la vie privée (e.g., violation de données, scandales liés à l'utilisation abusive de données). Les auteurs souhaitent

en faisant cela mesurer les répercussions financières pour les entreprises (et soulignent la nécessité de continuer les recherches portant sur les réponses des consommateurs). Notre typologie répond quant à elle à un souhait de faire ultérieurement le lien entre préjudices (Citron & Solove, 2021), réponses et dédommagements. C'est pourquoi notre recherche apporte une contribution théorique importante en matière de protection des consommateurs.

Par la suite, notre typologie pourrait être enrichie en intégrant de nouvelles solutions comme la *negociation, active-recommandation privacy policy application* (Liu et al., 2021) : cette solution permet aux agents de service clientèle de services bancaires de faire des recommandations personnalisées en matière de politiques de confidentialité.

De plus, notre typologie intègre un comportement spécifique de plainte : la plainte au régulateur, que nous détaillons maintenant, et qui pourrait par la suite être approfondie.

2.2. Compréhension d'un comportement de plainte spécifique : la plainte au régulateur

Notre recherche met en lumière un comportement spécifique de plainte : la plainte au régulateur (e.g., CNIL). À notre connaissance, ce comportement n'a jamais été étudié. Or il est rendu possible en Europe à travers le RGPD, offrant ainsi des possibilités de plaintes à 750 millions de personnes, et dans d'autres pays (e.g., en Californie avec le CPRA). Bien sûr, les nombreuses réglementations internationales en matière de protection de la vie privée qui apparaissent n'offrent pas toutes ces possibilités de plainte (e.g., en Chine). Ce comportement de plainte semble aussi un bon indicateur de la maturité en matière de cybersécurité d'une population. Par exemple, les experts du cabinet DLA Piper expliquent l'augmentation récente du nombre de plaintes déposées au régulateur en Pologne¹²¹ par une plus grande sensibilité de la population aux risques de cybersécurité.

Comme nous l'avons indiqué en discussion de l'essai macro, certains points de vigilance s'imposent dans l'exploration de ce comportement de plainte : (i) le nombre de plaintes, même s'il est en progression, reste faible en comparaison avec le nombre d'atteintes à la vie privée et

¹²¹ Generalny Inspektor Ochrony Danych Osobowych (www.giodo.gov.pl)

de violations de données personnelles¹²² ; (ii) le nombre de plaintes doit être mis au regard des motifs de plaintes (inconnus à ce jour de notre part) ; (iii) le nombre de plaintes doit être mis au regard de la situation des pays européens, notamment la proximité géographique avec les centres décisionnels ou la facilité de dépôt de plainte.

Enfin, en vue d'un dédommagement des individus et des consommateurs à la suite d'une violation de données personnelles, des interrogations résident dans l'intérêt des dépôts de plainte. Nous discutons ce point plus particulièrement dans les contributions pratiques de notre recherche.

3. Distance psychologique avec la protection de la vie privée

Notre recherche confirme les travaux récents sur le concept de distance psychologique avec la vie privée (Bandara et al., 2018; Bandara et al., 2021; Hallam & Zanella, 2017), et les complète.

Premièrement, comme pour ces travaux (Bandara et al., 2018; Bandara et al., 2021), nous utilisons les différentes dimensions (sociale, hypothétique, spatiale, temporelle) de la distance psychologique (Trope & Liberman, 2010). Nos résultats interrogent de ce fait le rôle de la distance temporelle, qui semble ne pas être significatif, contrairement au cas du changement climatique et aux hypothèses de Bandara et al. (2021).

Deuxièmement, nous appliquons la distance psychologique à un autre contexte : les violations de données personnelles. Notre recherche permet d'avancer des éléments pour la définition d'une échelle de mesure de la distance psychologique avec la violation de données personnelles.

Troisièmement, notre recherche apporte un éclairage nouveau sur le construit avec lequel nous cherchons à mesurer la distance psychologique, qu'il faudra ensuite chercher à réduire pour agir. Pour illustrer notre propos, nous nous référons aux travaux qui se sont intéressés au changement climatique. Ces derniers ont identifié la réduction de la distance psychologique comme un levier efficace pour activer des actions de prévention face au réchauffement climatique (Brügger et al., 2016; Singh et al., 2017; Spence et al., 2011, 2012). En effet, dès

¹²² Rapport Institut Montaigne décembre 2019 « Données Personnelles, comment gagner la bataille ? », disponible à : <https://www.institutmontaigne.org/ressources/pdfs/publications/donnees-personnelles-comment-gagner-la-bataille-etude.pdf>

2010, les discours médiatiques sur le changement climatique ont fait le lien, par exemple, avec les phénomènes de fonte des neiges ou de disparition de certaines espèces animales et amené le public à mieux s'identifier et s'intéresser à la cause. Le terme « changement climatique » nous semble, à ce jour, plus concret que celui de « risques pour la vie privée ». De fait, les risques liés à la violation de la vie privée restent peu connus (en France en janvier 2023, 42% des internautes se soucient de l'usage de leurs données personnelles par les grandes entreprises vs. une moyenne mondiale à 32%¹²³).

Quatrièmement, nous montrons que la distance psychologique avec les violations de données personnelles a une influence plus importante que la préoccupation pour la protection des données personnelles. Ainsi, la perception des risques de cybersécurité amène à être plus actif. Cela est, d'ailleurs, concordant avec certaines observations ¹²⁴ qui expliquent les augmentations du nombre de plaintes au régulateur dans certains pays (e.g. Pologne) par une prise de conscience importante des risques de cybersécurité.

Enfin, nous mettons en lumière le fait que la distance psychologique est un mécanisme pertinent pour relier effets culturels et réponses face aux violations de données personnelles. Une exploration en profondeur des différentes dimensions de la distance psychologique s'impose, à la fois dans le lien entre orientations culturelles et dimensions de la distance psychologique (e.g., lien entre distance sociale et relation à l'*endogroupe* et à l'*exogroupe*) que dans le lien entre dimensions de la distance psychologique et types de réponses (e.g., quel impact de la distance hypothétique sur les différents types de réponses ?). Ceci permettrait notamment de mieux comprendre le rôle de la culture dans les représentations mentales (Shapira et al. 2012), alors que trop peu d'études s'intéressent à l'influence des variations culturelles dans les processus cognitifs (Wiesenfeld et al., 2017).

¹²³ Etude de wearesocial disponible à : <https://wearesocial.com/uk/blog/2023/01/digital-2023/>

¹²⁴ DLA Piper GDPR fines and data breach survey. *op. cit.*

4. Théorie de la pratique et pratiques de protection de la vie privée

Notre recherche a permis d'identifier un nouveau cadre théorique, que nous mettons au regard des principaux cadres théoriques utilisés dans les recherches en vie privée (4.1.). La théorie de la pratique aide à mieux éclairer les phénomènes méso des mécanismes de protection de la vie privée, qui apportent une meilleure compréhension des mécanismes reliant les cadres macro et micro mais aussi des phénomènes d'engagement et de résistance (4.2.).

4.1. Nouveau cadre théorique appliqué à la protection de la vie privée

Comme nous l'avons montré page 103, la protection de la vie privée a été observée selon trois angles (Martin & Murphy, 2017) : économique et organisationnel (les données personnelles étant considérées comme un actif), psychologique (à travers les raisons et impacts attitudinaux et comportementaux de la préoccupation pour la protection de la vie privée) et sociétal (en distinguant d'une part les impacts cross-culturels et internationaux, et d'autre part les impacts éthiques et réglementaires). En somme, la protection de la vie privée est vue soit de façon macro (économique, institutionnelle, internationale) soit de façon micro. Ainsi les cadres théoriques utilisés concordent avec cette approche (cf. Figure 10, Li, 2012), avec pour exemples la théorie de l'espérance d'utilité (visée économique), la théorie de l'agence (visée institutionnelle), ou la théorie de l'action raisonnée (visée psychologique).

Récemment Quach et al. (2022) ont utilisé la théorie de la structuration (Giddens, 1984) pour expliquer que les tensions liées à la protection de la vie privée (violations de données ou scandales liés à une utilisation frauduleuse de données) résultent des interactions entre les entreprises et les consommateurs. Mais les réponses des acteurs sont formulées indépendamment, n'identifiant pas la pratique en elle-même, fruit d'interactions à un niveau méso.

Si certaines théories ont pu être mobilisées à un niveau méso (e.g., social presence theory), Li (2012) souligne un manque de compréhension des phénomènes sociologiques et recommande de croiser les cadres conceptuels mobilisés à un niveau macro, méso et micro, afin de faire émerger de nouvelles idées. Alors que notre recherche envisage la protection de la vie privée comme une pratique sociale, nous sommes alors heureux de constater qu'elle ait pu offrir un éclairage sociologique novateur.

À notre connaissance, aucun éclairage sociologique considérant la préoccupation pour la protection de la vie privée comme un phénomène sociologique, un objet à part entière, indépendamment des agents n'a été à ce jour apporté. Ceci est assez étonnant alors que la vie privée, indépendamment de toute considération numérique ou digitale, a souvent été expliquée comme un phénomène sociologique (Schwartz, 1968), résultant d'une adaptation à un contexte donné, comme une vie nomade ou des logements exigus (Ariès & Duby, 1985). De fait, notre recherche complète les précédentes recherches.

4.2. Compréhension des phénomènes de changement, d'engagement et de résistance

4.2.1. Compréhension des phénomènes reliant macro et micro

La théorie de la pratique a été beaucoup utilisée pour expliquer les changements technologiques (Kuhlmann & Rip, 2019; Rip & Kemp, 1998) et les modifications pro-environnementales (Shove, 2010, 2011; Shove et al., 2012). Ces travaux montrent que l'observation du niveau méso permet de rendre compte des effets et des changements. La politique n'a pas de rôle particulier dans les changements technologiques, à part être une force externe façonnant les voies de l'innovation. Les changements se font par l'interaction de valeurs, de matériaux et de formes de compétences : c'est pourquoi dans certaines parties du monde, les pratiques fonctionnent mais dans d'autres, ce n'est pas le cas car les éléments nécessaires (pour les pratiques) ne sont pas là. Ainsi, la théorie de la pratique ne traite pas des explications du changement à plusieurs niveaux ni comme étant des phénomènes à des niveaux différents et indissociés : les pratiques se combinent, évoluent et disparaissent, dans des cadres spatiaux et temporels.

Comprendre la protection de la vie privée comme une pratique sociale permet de mettre en lumière l'importance des niveaux d'observations méso : organisations, entreprises et collectifs. Cela permet aussi de minimiser l'importance des idéaux au bénéfice des matériaux et compétences. Les orientations en matière de protection des données personnelles dans certains groupes sociaux (comme les familles modestes ou les milieux ruraux ; Pasquier, 2018) ou dans des pays comme l'Inde, la Chine et d'autres pays émergents (Martin & Murphy, 2017) peuvent

s'expliquer par d'autres facteurs comme la distance psychologique avec les risques de sécurité informatique ou l'alphabétisation numérique.

De plus, une compréhension des phénomènes à un niveau méso permet l'identification des réponses entre des cadres macro et micro, comme nous l'avons déjà vu, mais également interroge sur les questions d'engagement et de résistance dans les changements technologiques (au sein desquels la question de la protection des données personnelles s'inscrit).

4.2.2. *Théorie de la pratique, effets d'engagement et de résistance*

La décision d'agir pour la protection de la vie privée résulte souvent d'un compromis entre une action civique (*civic agency*), en tant que citoyens, et une action quotidienne (*market agency*) en tant qu'acteurs ou consommateurs (Chaudhury & Albinsson, 2015). Cette tension citoyen-consommateur se situe entre les macro-pouvoirs des institutions (contrôle de la réglementation de la protection des données personnelles et de l'économie numérique) et le micro-pouvoir individuel (gestion des données personnelles). Elle se traduit par un écart entre les besoins de la société au niveau macro et ceux des consommateurs au niveau micro (Valor et al., 2017). Ne pouvant avoir une influence immédiate et réelle au niveau macro (réglementation et économie numérique), les individus cherchent à avoir un rôle au niveau méso (e.g., groupes sur les réseaux sociaux pour échanger des « trucs et astuces » pour se protéger en ligne, ou les associations militantes). En particulier, les changements sociétaux résident essentiellement dans les liens de causalité à un niveau méso (Johnson & Schaltegger, 2020), les associations et les groupes sociaux contribuent aux orientations de la société, par le développement d'idées et de référentiels, et où des dynamiques collectives se développent (Chognot, 2020).

Le cadre de la théorie de la pratique permet ainsi de mieux identifier les comportements d'engagement et de résistance aux risques liés à la protection de la vie privée. Ceux-ci peuvent s'inscrire dans un cadre plus large de résistance aux technologies : récemment, Chamaret et al. (2020) ont montré que les risques nouveaux tels que les potentielles violations de vie privée et le piratage informatique freinaient l'adoption de compteurs électriques au niveau des municipalités. Un meilleur accompagnement au niveau des collectivités sur les risques liés aux violations de vie privée (cf. implications pratiques) pourrait accompagner ces démarches.

5. Nouvelle compréhension du souci de protection de la vie privée

La préoccupation pour la protection de sa vie privée s'exprime par le contrôle de ses données personnelles. Le contrôle de ses données personnelles est un droit individuel, fondé sur le contrôle et donc la confiance et la transparence. À la lumière de nos résultats, nous discutons les fondements individuels du souci de contrôle des données personnelles (5.1.), les limites d'une sur-individualisation du contrôle des données personnelles (5.2.) et la perte de contrôle et de transparence dans une situation de vulnérabilité informatique (5.3.). Ceci nous amène à proposer une nouvelle définition basée sur le souci de sécuriser les données personnelles de tous (5.4.).

5.1. Fondements individuels du souci de contrôle des données personnelles

À travers nos trois essais, nous avons montré qu'une préférence culturelle pour des valeurs d'équité sociale et de genre amène les individus à être plus actifs dans les réponses apportées face à des violations de données personnelles. Cela remet en question le rôle de l'individualisme comme valeur fondatrice du droit à la protection de la vie privée. Comme un répondant dans l'essai méso l'a verbalisé : « ma liberté m'importe peu si elle n'est pas celle de tous ». Ce nouvel éclairage culturel fait la lumière sur les motivations profondes (individuelles ? ou collectives ?) du droit à la vie privée : nous les discutons ci-dessous.

Nous souhaitons inviter la communauté à s'interroger sur les fondements du souci de contrôle de ses données personnelles. Premièrement, comme déjà mentionné, la préoccupation pour la confidentialité de la vie privée est définie comme le droit de contrôler l'accès à ses propres informations personnelles et le partage de celles-ci avec des tiers (Belanger et al., 2002), dans un contexte de collecte accrue de données personnelles. De façon plus large, le souci de contrôle de ses données personnelles est l'expression d'un droit universel à la protection de la vie privée (article 12 de la Déclaration universelle des droits de l'homme) instauré en période post Seconde Guerre mondiale pour protéger un chacun des immixtions dans sa vie privée, et donc avec des objectifs de sécurité, de protection des démocraties et de la vie en communauté. Les motivations ne sont donc pas individuelles.

Deuxièmement, le souci de contrôle de ses données personnelles répond à une volonté de protection de sa vie privée. La protection de la vie privée existe dans tous les contextes et les cultures : « *la vie privée est un processus universel qui implique des mécanismes de régulation*

propres à chaque culture » (Altman, 1977, p.66). Or de tout temps, la régulation de la vie privée a pour objectif de permettre la vie en communauté (Ariès & Duby, 1985). À nouveau, les motivations ne sont pas individuelles.

5.2. Limites d'une sur-individualisation du contrôle des données personnelles

Dans la continuité du paragraphe précédent, et sur la base de nos résultats, prônant une préférence culturelle à une équité sociale, nous interrogeons non seulement les motivations profondes du droit à la vie privée, mais également les moyens de recours à ce droit. En particulier, si les motivations de la protection de la vie privée sont collectives, les moyens de recours à ce droit ne doivent-ils pas l'être également ? De plus, les résultats obtenus dans l'essai méso montrent également la nécessité de moyens de réponses plus collectifs : soit il est complexe de recourir à des moyens techniques (e.g., compétences techniques, barrière de la langue anglaise), soit les réponses institutionnelles sont peu efficaces, laissant la place à des réponses sociales fondées sur des dynamiques collectives.

Par conséquent, nous souhaitons mettre ces résultats au regard de précédents travaux interrogeant les limites d'une sur-individualisation du contrôle des données personnelles à travers : (i) la difficulté pour les individus à faire des choix sur leur vie privée, (i) le paradoxe de la vie privée, (ii) une vulnérabilité incontrôlée de l'individu.

En effet, le principe d'autonomie et de responsabilisation des individus vis-à-vis de leurs données personnelles est remis en question. Il suppose que les individus fassent des choix et des calculs concernant leur vie privée (*privacy calculus*). Or ce calcul est complexe pour plusieurs raisons : (i) une asymétrie informationnelle entre consommateur et organisation, i.e., un décalage d'informations sur les coûts et bénéfices d'un partage d'informations (Rochelandet, 2010) ; (ii) des distorsions psychologiques comme le biais d'optimisme (Acquisti, 2004) ; (iii) du niveau d'abstraction du concept de préoccupation pour la vie privée qui amène à un certain décalage entre bénéfices concrets et immédiats (e.g., personnalisation de services ou satisfaction individuelle ; Cloarec, 2020) et risques hypothétiques. Cela implique un paradoxe de la vie privée (*privacy paradox*) (Pavlou, 2011), i.e., un décalage paradoxal entre les

préférences déclarées en matière de protection de la vie privée et le comportement réel en termes de divulgation de la vie privée (Aguirre et al., 2015 ; Norberg et al., 2007).

Le paradoxe de la vie privée est également remis en question, parce que trop simpliste dans l'analyse des comportements. Plusieurs alternatives sont proposées : (i) le paradoxe de la vie privée devrait être un paradoxe de la confiance, entre la confiance accordée avec émotion aux communautés et la confiance accordée rationnellement aux institutions (Lutz & Strathoff, 2014) ; (ii) la notion de vie privée doit être séparée de la notion de risques en distinguant le *privacy calculus* (i.e., l'arbitrage entre des bénéfices attendus et des risques liés à la vie privée) du *risk calculus* (i.e., l'arbitrage entre des risques liés à la vie privée et l'efficacité des mécanismes d'adaptation) (Li, 2012).

Par conséquent, l'individu est-il vraiment en mesure d'être responsable du contrôle de ses données personnelles ? Son incapacité à en être responsable n'est-elle pas accrue dans un contexte de violations de données personnelles ? Les recherches récentes soulignent d'ailleurs le contexte de vulnérabilité (i.e., la perte de liberté et de contrôle) dans lequel se trouvent les personnes (Del Bucchia et al., 2021; Brough & Martin, 2021; Cloarec, 2022) ?

5.3. Pertes de contrôle et de transparence : réponses du consommateur en situation de vulnérabilité informatique

Les résultats obtenus dans l'essai micro montrent que le souci de contrôle de ses données personnelles (exprimé par exemple à travers l'item « mes données personnelles sont partagées avec des tiers sans mon accord ») a une influence moins importante que la distance psychologique avec les violations de données personnelles. La capacité de contrôle de ses données est moins perçue. Quasiment tous les répondants dans l'essai méso déclarent ne rien pouvoir faire et contrôler face à une violation de données personnelles.

Dans ce dernier paragraphe, nous souhaitons ouvrir une discussion sur le cadre dans lequel les réponses face aux violations de données doivent être abordées :

- Les réponses doivent-elles être considérées comme des plaintes relativement rationnelles et responsables du consommateur, inscrivant alors les travaux sur ce champ dans la continuité de ceux en *consumer complaint behaviour* ?
- Ou bien est-il nécessaire de mettre en lumière la vulnérabilité du consommateur ?

Les travaux considèrent les violations de données personnelles comme des incidents de service (e.g., Rasoulzadeh et al., 2021), dans un cadre de contrat social implicite entre un consommateur et une entreprise, fondé sur des principes de transparence et de contrôle des données (que nous avons explicités par ailleurs). Cela implique une transparence à toutes les étapes du processus. Or les entreprises déclarent-elles tout le temps et immédiatement les violations de données dont elles font l'objet ? Et les autorités européennes ont-elles tous les moyens de contrôler ces déclarations ?

Deuxièmement, cela implique également des possibilités de contrôle à toutes les étapes du processus. Or, à la suite à la notification d'une violation de données, comme nous l'avons démontré, les possibilités de plainte et de recours sont très complexes comme nous l'avons montré. Les consommateurs peuvent changer d'enseignes (Grosso et al., 2020) ou exprimer leur mécontentement à travers une baisse de confiance qui impacte les cours boursiers. Mais cela règle-t-il vraiment le problème ? Nos résultats semblent montrer que la réponse majoritaire est la *loyalty*, i.e., l'absence d'alternative abordable, ou la résignation (Hirschman, 1970).

Troisièmement, s'agit-il d'un incident de service ou d'une faille de sécurité plus large et qui dépasserait les entreprises ? Quelles sont les possibilités des petites et moyennes entreprises

face aux cyberattaques et aux demandes de rançon ? Pour faire écho à notre premier exemple cité en introduction de cette thèse, quelles sont les possibilités des centres hospitaliers face aux demandes de rançon de pirates informatiques (impliquant alors qu'il s'agit d'un non-respect du secret professionnel et médical plus que d'un incident de service) ?

Quatrièmement, certaines violations de données sont provoquées par une action sur un lien frauduleux dans un e-mail (*fishing*). Les consommateurs peuvent-ils être considérés comme responsables ? Peut-on considérer qu'ils aient consenti au partage de leurs informations ?

Par conséquent, nous remettons en question les principes de transparence et de contrôle dans le cadre des violations de données personnelles. Cela a plusieurs conséquences théoriques :

- Une nouvelle compréhension du lien entre vie privée et sécurité. Nous souhaitons en ce sens approfondir la notion de vulnérabilité informatique du consommateur ;
- Un partage des responsabilités, en déresponsabilisant l'individu (et donc en modifiant les moyens de recours au droit et les principes de self-data management) et en surresponsabilisant les entreprises et les différents acteurs (à travers le développement de pratiques).

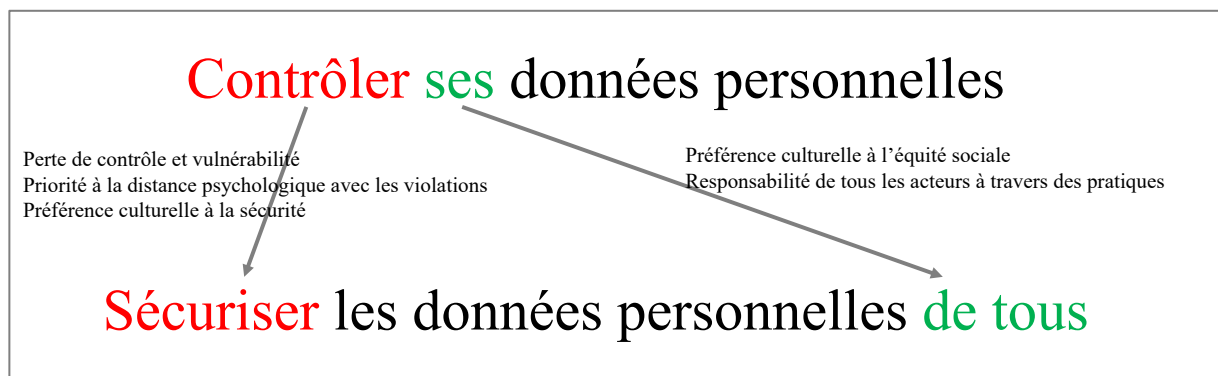
5.4. Proposition de nouvelle définition pour la protection de la vie privée

En conclusion nous proposons de définir la préoccupation pour la protection privée, non plus comme le souci de contrôle de ses données personnelles mais comme le **souci de sécuriser les données personnelles de tous** : cf. Figure 43.

Face aux violations de données personnelles, le contrôle des données ne semble plus possible, mettant l'individu dans une situation de vulnérabilité. Communiquer sur des notions de sécurité et sur une réduction de la distance psychologique avec les violations de données personnelles est plus efficace. Par conséquent, sécuriser vaut mieux que contrôler.

Par ailleurs, la mise en lumière de l'importance des valeurs d'égalité sociale et de genre permet d'éclairer une compréhension de la préoccupation pour la vie privée, établie dans un souci de « mieux vivre ensemble » (et non de « mieux vivre tout seul »). Ceci s'exprime également par une responsabilité des acteurs à travers le développement de pratiques de protection de la vie privée.

Figure 43 : Proposition de définition pour la protection de la vie privée



Et après ? Sur la base de cette définition, nous proposons dans la partie suivante différentes implications pratiques autour de trois propositions :

- Accentuer le niveau méso et adopter une « approche terrain », avec une importance et des moyens accordés aux collectivités, écoles, structures éducatives, associations ;
- Développer la responsabilité des entreprises et de bonnes pratiques chez tous les acteurs,
- Renforcer les discours médiatiques sur les notions d'équité et de sécurité ;
- Renforcer les possibilités de plaintes collectives (ceci en réponse à l'appel de Dinev (2014) à des analyses anthropologiques et culturelles différentes de la vie privée, permettant d'optimiser les approches régulatrices en la matière).

Section 2. Implications pratiques

Cette troisième section est consacrée à l'identification de recommandations concrètes. Dans la Figure 42 page 345, nous avons précisé les implications pratiques de nos recherches selon les trois axes de résultats :

- Sur la base de nos résultats portant sur les réponses face aux violations, favoriser (i) les possibilités de plaintes aux régulateurs et (ii) la responsabilité des entreprises dans l'identification des violations, (iii) identifier les améliorations possibles pour chaque réponse ;
- Pour prendre en compte les effets culturels identifiés (équité, liberté, sécurité), (i) développer des actions de communication, (ii) développer des moyens d'action autour du « mieux vivre ensemble », (iii) adapter les moyens d'action selon les groupes sociaux, (iv) adapter localement les réglementations globales et développer des moyens de recours au droit plus collectifs ;
- Pour prendre en compte les mécanismes sociologiques et psychologiques, (i) développer une feuille de route basée sur la théorie de la pratique, (ii) développer des actions incluant la réduction de la distance psychologique.

Plutôt que d'énoncer ces différentes possibilités d'applications concrètes successivement, nous préférons apporter une vision globale et montrer que ces actions sont reliées et comment elles peuvent se coconstruire dans le temps. Ainsi nous présentons ces recommandations pratiques dans un cadre général basé sur la théorie de la pratique (1.). Nous donnerons ensuite quelques exemples de communication, qui s'appuient en particulier sur des possibilités de réduction de la distance psychologique (2.), et nous insisterons sur les modifications à apporter à nos réglementations (3.).

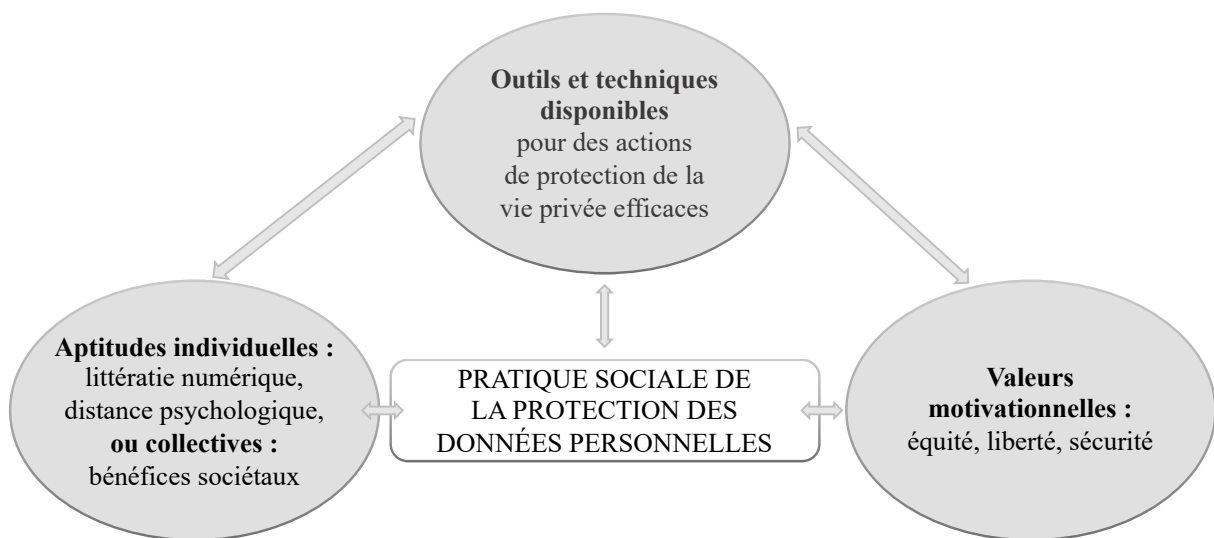
1. Développement de pratiques de protection de la vie privée

Dans ce paragraphe, nous reprenons ci-dessous les bases de la théorie de la pratique sociale de protection de la vie privée (1.1.), nous déroulons comment les trois briques de la théorie de la pratique (valeurs, matériaux, compétences) peuvent agir conjointement et s'appliquer concrètement (1.2.), nous identifierons plus succinctement les acteurs qui interviennent dans cette pratique et quelles peuvent être leurs actions (1.3.).

1.1. Structure de la pratique sociale de la protection de la vie privée

La pratique sociale de la protection de la vie privée se base sur une structure alliant valeurs (équité, liberté, sécurité), matériaux (outils et techniques de protection), formes de compétences (en particulier littératie numérique, distance psychologique et bénéfices sociétaux) (cf. Figure 44). Ces différents moyens d'action doivent se développer parallèlement et en étant interreliés, par différents acteurs, avec le passage d'une responsabilité individuelle à une responsabilité collective, basée sur une dynamique collective et une logique d'entraide.

Figure 44 : Structure de la pratique sociale de la protection de la vie privée



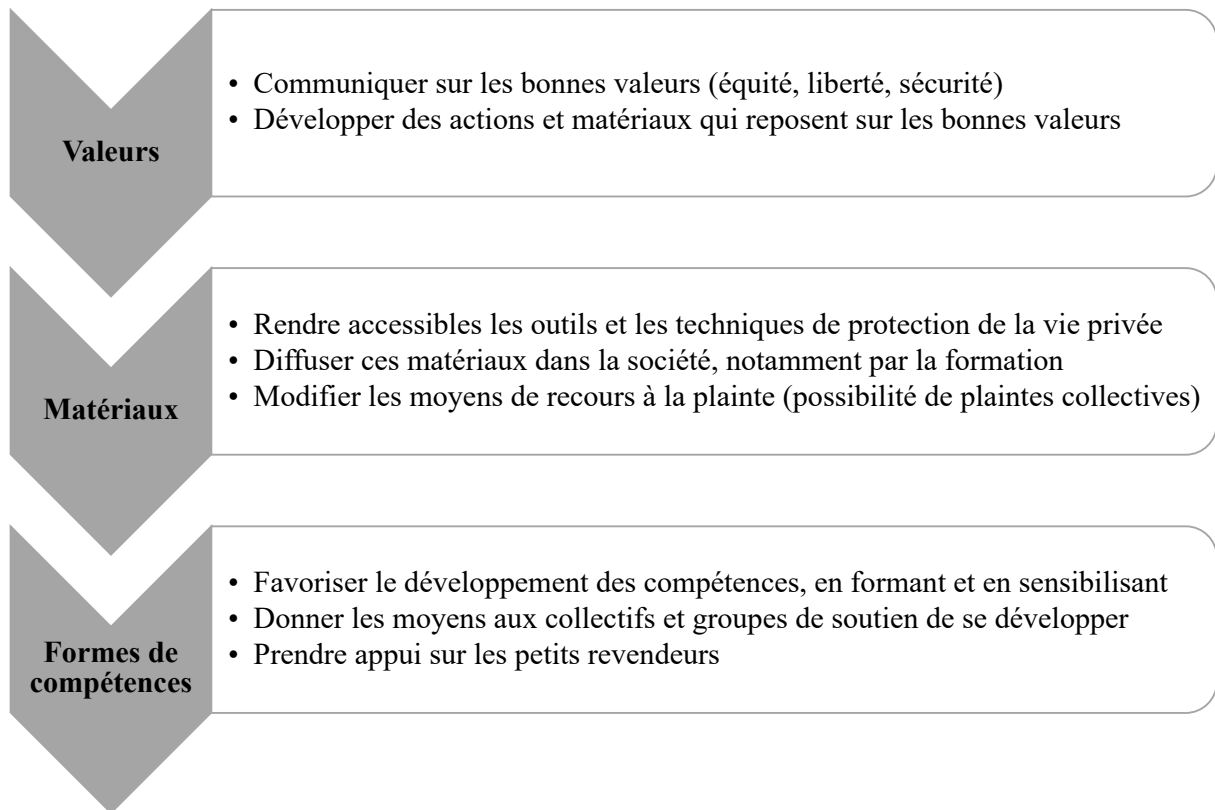
Nous précisons dans le paragraphe suivant plus concrètement comment ces éléments peuvent être appliqués.

1.2. Applications concrètes pour le développement de pratiques de protection de la vie privée

1.2.1. Identification d'actions concernant les valeurs, matériaux et formes de compétences

Dans notre démarche, nous reprenons nos trois axes de résultats (concernant les réponses, les effets culturels et les mécanismes psychologiques et sociologiques) et nous voyons comment ils peuvent être appliqués concrètement aux trois éléments de la structure ; i.e., valeurs, matériaux et formes de compétences. Plusieurs applications pratiques peuvent être développées, ce que nous précisons dans la Figure 45.

Figure 45 : Applications pratiques des éléments de la structure de la pratique sociale



En premier lieu, il s'agit de mobiliser les bonnes valeurs et les schémas motivationnels dominants (i.e., équité, liberté, sécurité) dans les communications et les actions. Comme nous le montrons dans le paragraphe 2.1., il nous semble plus efficace de parler de « sécurité » que de « protection de la vie privée ». Ceci peut également avoir un impact plus général sur les actions de protection et les moyens de recours au droit. Par exemple, la sensibilisation aux risques de cybersécurité et les discours médiatiques dans ce sens expliquent depuis 2020 en

partie l'augmentation du nombre de plaintes auprès des régulateurs en Pologne¹²⁵. Par ailleurs, les entreprises mobilisent souvent les discours de transparence afin d'assurer la confiance de leurs clients et consommateurs : dans une logique collective et de recherche d'équité sociale, il pourrait être plus pertinent de montrer comment accompagner les personnes en situation de vulnérabilité informatique. Les actions et les moyens de recours au droit doivent reposer sur des principes d'équité sociale, de liberté et de sécurité. Nous insisterons dans ce sens dans le paragraphe 3.3. sur les possibilités de plaintes collectives.

En second lieu, concernant les matériaux, il est nécessaire de rendre disponibles, accessibles et connus les outils et techniques (matériaux) nécessaires pour protéger sa vie privée, que ce soit des moyens techniques ou des moyens de recours au droit.

En dernier lieu, concernant les formes de compétences, il est impératif de développer les formes de compétences (individuelles ou collectives) qui sont autant de freins ou d'accélérateurs au développement de bonnes pratiques.

1.2.2. Actions qui agissent conjointement

Comme nous l'avons stipulé dans la partie sur les contributions théoriques, les trois éléments de la structure agissent conjointement. Dans notre exemple, le développement de la marche nordique en dehors de la Finlande ne s'est pas fait par l'unique distribution de bâtons de marche par de grandes enseignes de sport, mais par la circulation d'images, de formes de compétences, de référentiels. De même, si les idéaux amènent un individu à vouloir pratiquer la marche nordique, ils vont évoluer au fur et à mesure de la pratique ; et l'usage du bâton de marche a une influence sur la perception que l'utilisateur en a et sur ses formes de compétences.

Dans notre contexte, l'ensemble des actions concrètes envisagées ne peuvent pas être imaginées indépendamment : les propositions faites pour les discours publicitaires et médiatiques peuvent avoir un impact sur l'usage d'outils mobilisés face à une violation de données personnelles et l'usage de moyens de recours au droit influence les formes de compétences. Aussi un travail plus approfondi pourrait être mené pour mieux comprendre cet entrelacement des actions.

¹²⁵ DLA Piper GDPR fines and data breach survey. *op. cit.*

1.2.3. Dynamique basée sur le méso

Pour l'ensemble des actions énoncées dans la Figure 45, plusieurs acteurs interviennent que nous précisons dans le paragraphe suivant. Pour chaque acteur, nous proposons plusieurs actions envisagées et envisageables : en effet, de nombreuses actions existent déjà (nous les citons succinctement), nous les complétons.

Notre objectif est essentiellement de montrer que ces actions doivent être centrées sur des niveaux méso : collectifs, associations, collectivités territoriales, et surtout entreprises. Comme nous l'avons expliqué dans la partie sur les contributions théoriques, c'est l'effet méso qui est à l'origine de tout. La protection de la vie privée doit donc sortir d'un cadre réglementaire et très « descendant », un pouvoir et des moyens plus importants doivent être confiés aux associations et aux collectifs, les entreprises doivent jouer leur rôle central économique et social. Par un effet de ruissellement, les effets et les structures sociales vont ensuite d'une part être intégrés par les individus et d'autre part reprises et intégrés au niveau macro (institutionnel et réglementaire). De même, notre objectif est d'inscrire les actions dans une approche concentrée autour du développement de pratiques, afin que chaque individu puisse se les approprier pour en faire une routine. Pour cela, il faut laisser le temps aux pratiques de se développer.

Il existe un sentiment de perte d'efficacité dans la transmission entre les niveaux méso et macro, et plus particulièrement entre les collectifs et la CNIL, qui ressort d'une part des entretiens que nous avons effectués (cf. Tableau 42) et d'autre part de plusieurs tables rondes initiées par la CNIL avec des représentants d'associations :

- En page 3 du rapport¹²⁶ : « Les associations perçoivent la CNIL comme un acteur à faire bouger dans le sens de leur engagement, de plusieurs manières : par la critique et l'interpellation publique, ou par l'échange, formel ou informel. Ces modes d'actions sont complémentaires les uns des autres et chaque association peut avoir recours à une ou plusieurs formes à la fois. Les associations peuvent également inviter la CNIL à leurs événements »,
- ou encore en page 4 du même rapport : « d'un côté la société civile peut permettre à la CNIL d'avoir une meilleure compréhension de ce qui se passe sur le terrain en

¹²⁶ Rapport « Atelier CNIL Associations de défense des droits et libertés, partenariat pour un gouvernement ouvert » disponible à : <https://www.cnil.fr/fr/faire-dun-droit-individuel-un-sujet-collectif-rencontres-entre-la-societe-civile-et-la-cnil-autour>

remontant les pratiques et problèmes observés ainsi que jouer le rôle de lanceur d’alerte. Par exemple, l’expérience qu’ont des associations dans l’exercice des droits pourrait aider à définir les problèmes courants qui pourraient être utilisés pour mettre à jour le processus et le parcours de plaintes pour les plaignants. De son côté, la CNIL a une vision d’ensemble et une forte expertise à partager avec la société civile pour les aider à structurer leurs actions et à formuler des réponses »

- et enfin en page 7: « Certaines associations constatent que le dialogue existe déjà, ou a déjà existé, mais que la plupart du temps cela ne va pas plus loin : il existe un sentiment de perte dialogue lorsque l’on sort des échanges avec le LINC ».

De la même manière, les entreprises et les structures éducatives ont un rôle central car l’adoption des supports informatiques se fait souvent à l’école ou au travail : nous repreciserons ce point dans le paragraphe suivant.

La recommandation centrale de notre recherche est d’accroître les efforts sur les niveaux méso de notre société : structures éducatives et écoles d’une part, entreprises d’autre part, collectifs et associations enfin. Des actions « avec une approche terrain » favoriseront cela.

Par un effet de ruissellement et à travers le développement de pratiques, les moyens de protection de la vie privée seront adoptés comme des routines par les individus et intégrés par les institutions.

1.3. Acteurs de la pratique sociale de la protection de la vie privée

Nous identifions plusieurs acteurs intervenant dans la structure du développement d'une pratique sociale de la protection de la vie privée : les entreprises, les instances politiques et régulatrices (CNIL et Commission européenne), les acteurs de la cybersécurité (ANSII), les structures éducatives et les établissements scolaires, les collectivités locales et territoriales, les structures associatives et la société civile. Nous illustrons dans le Tableau 58 ci-après plusieurs actions qui pourraient être développées par chacun de ces acteurs, que nous précisons ensuite pour certaines.

De façon générale, les actions des acteurs reposent sur 4 leviers : (i) communiquer, (ii) former et développer des compétences, (iii) faciliter les moyens de recours et (iv) être un support collectif.

Tableau 58 : Acteurs de la pratique sociale de la protection de la vie privée

Acteurs	Actions
Entreprises	- Accès aux outils, développement de bonnes pratiques - Responsabilité dans la protection contre les violations - Développement d'une organisation « privacy-centric »
CNIL et Commission européenne	- Communiquer - Développement des recours au droit collectif - S'appuyer sur un maillage local (représentant local de la CNIL)
Acteurs de la cybersécurité (ANSII)	- Communiquer - Former - Améliorer et diffuser des outils protecteurs (cf. Tableau 38, p.245)
Structures éducatives et établissements scolaires	- Renforcer les formations dès les écoles primaires et les certifications obligatoires - Interdire l'accès à des outils non réglementaires
Collectivités locales et territoriales	- Diversification des actions selon les bassins de population - Renforcer les actions contre la fracture numérique
Structures associatives	- Sensibiliser (mettre l'exemple d'UFC-Que choisir) - Être proche
Société civile	- S'appuyer sur tous les points de relais (ex. Fnac - revendeurs)

Notre objectif n'est pas de faire une présentation exhaustive de ces actions. Nous les expliquons rapidement dans les paragraphes suivants et les illustrons à travers quelques exemples.

La formation et l'éducation sont des éléments essentiels pour développer la littéracie numérique et de pratiques de protection de la vie privée. Pour cela, nous citons plusieurs pistes d'actions :

- renforcer les certifications PIX. En effet, la certification PIX est obligatoire pour tous les élèves de la 3^{ème} à la Terminale et l'ANSSI a contribué à la mise en place dans PIX d'un référentiel des compétences en cybersécurité ¹²⁷. Au regard des enjeux, il est probablement nécessaire de les renforcer ;
- développer les formations dès les classes primaires (comme les formations à la sécurité routière), dans un contexte où les enfants ont accès aux réseaux sociaux en moyenne vers l'âge de 8 ans et demi ¹²⁸ ;
- former les enseignants aux bonnes pratiques, les sensibiliser à leurs responsabilités de confidentialité des notes et appréciations de leurs élèves, leur donner accès aux bons outils, interdire certains outils types Google Classroom (cf. Figure 46 page 372) sans garantie absolue du respect des obligations de confidentialité et du respect de la protection des données personnelles ;
- s'appuyer sur les associations locales pour l'ensemble de ces actions ;
- intégrer les entreprises dans l'ensemble de ces actions ;
- enfin éduquer les pouvoirs publics, comme le recommande le rapport Bothorel¹²⁹ : « la fonction publique a besoin d'une culture de la donnée et du code. Ce besoin fait partie de ceux qui ont été le plus mis en avant par la consultation publique »).

¹²⁷ <https://www.ssi.gouv.fr/actualite/former-et-sensibiliser-a-la-securite-du-numerique-un-enjeu-strategique-pour-lanssi/>

¹²⁸ <https://www.vie-publique.fr/loi/288274-reseaux-sociaux-majorite-numerique-15-ans-proposition-de-loi#:~:text=D'apr%C3%AAs%20une%20enqu%C3%AAt%20de,seraient%20pr%C3%A9sents%20sur%20ces%20plateformes.>

¹²⁹ Rapport de la mission Bothorel, p.12, rapport disponible à : <https://www.vie-publique.fr/en-bref/277963-rapport-bothorel-pour-une-nouvelle-ere-de-la-politique-de-la-donnee>

Adopter une approche « terrain » est un élément essentiel du développement de dynamiques collectives des pratiques de protection de la vie privée. Cela est également nécessaire afin de diversifier les actions selon les bassins de population : notre recherche a en effet montré des variations d'orientations culturelles au sein d'un même pays, en réponse aux recherches actuelles sur la fracture numérique ; Pasquier, 2018). Pour cela, nous citons plusieurs pistes d'actions :

- SOS Tech¹³⁰ (cf. Figure 47 page suivante) est une entreprise engagée contre la fracture numérique, intervenant auprès des collectivités et administrations, acteurs de l'insertion professionnelle, seniors et particuliers. Nous pensons que ce type d'entreprises doit se multiplier mais aussi être mobilisé pour la protection de la vie privée ;
- Dans un second rapport issu des consultations de la CNIL, les associations proposent leur support (cf. page 3 du rapport des ateliers CNIL¹³¹) : « les associations dans leur ensemble peuvent agir par la sensibilisation du grand public aux enjeux du numérique et au logiciel libre, par l'affichage dans les médiathèques, par la participation à des colloques et conférences, par l'organisation d'ateliers. Elles s'appuient pour cela sur des groupes locaux (April par exemple). » ;
- Les revendeurs de matériel informatique peuvent aussi être de bons points de relais de bonnes pratiques en matière de protection de la vie privée. Cela peut être des magasins généralistes (Fnac) ou spécialisés (Cdiscount) mais également des petits revendeurs et réparateurs de smartphones et ordinateurs (leur rôle dans la société a été observé par l'anthropologue Nicolas Nova¹³² et ¹³³).

¹³⁰ <https://sostech.fr/>

¹³¹ Rapport « Atelier CNIL Associations du libre et de l'open source, partenariat pour un gouvernement ouvert » disponible à : <https://www.cnil.fr/fr/faire-dun-droit-individuel-un-sujet-collectif-rencontres-entre-la-societe-civile-et-la-cnil-autour>

¹³² Podcast «Le code a changé » épisode accessible à : <https://www.radiofrance.fr/franceinter/podcasts/le-code-a-change/smartphones-eloges-de-la-reparation-7598912>

¹³³ <https://curiousrituals.wordpress.com/>

Figure 46 : Exemple de Google Classroom

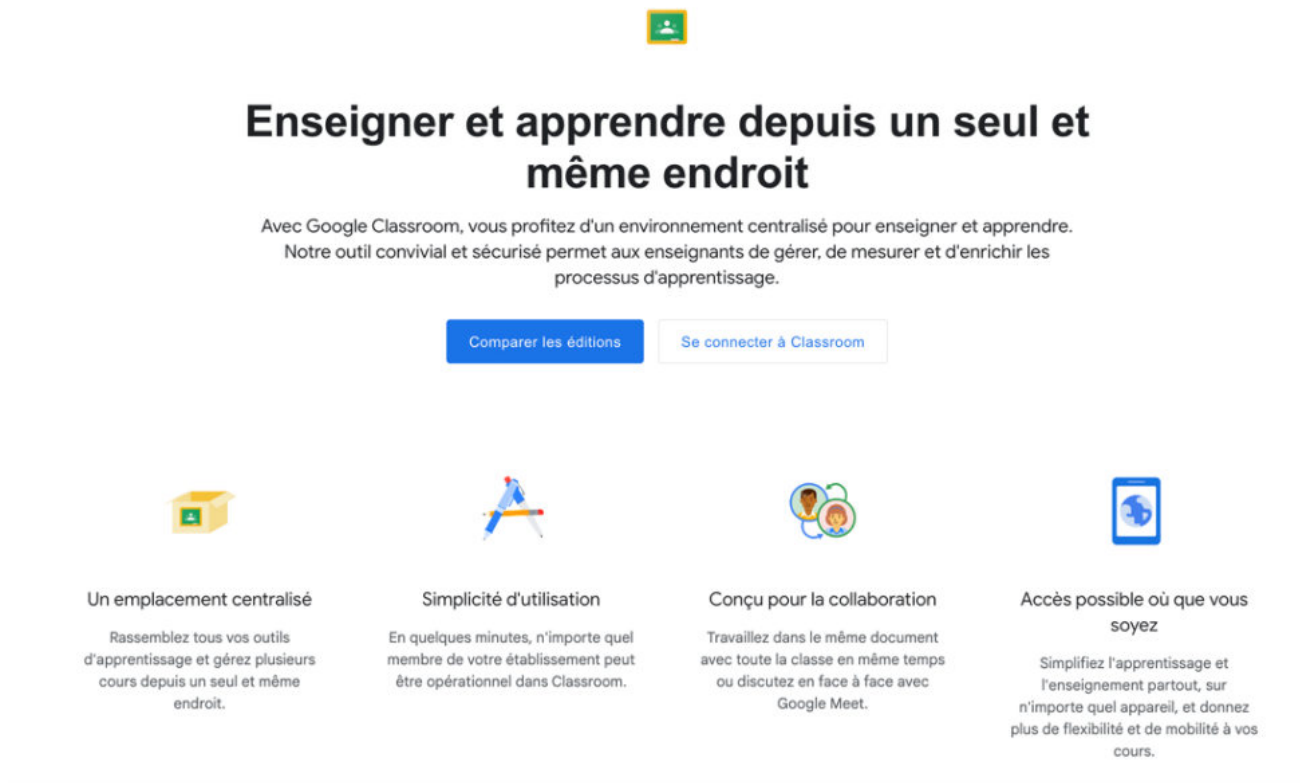
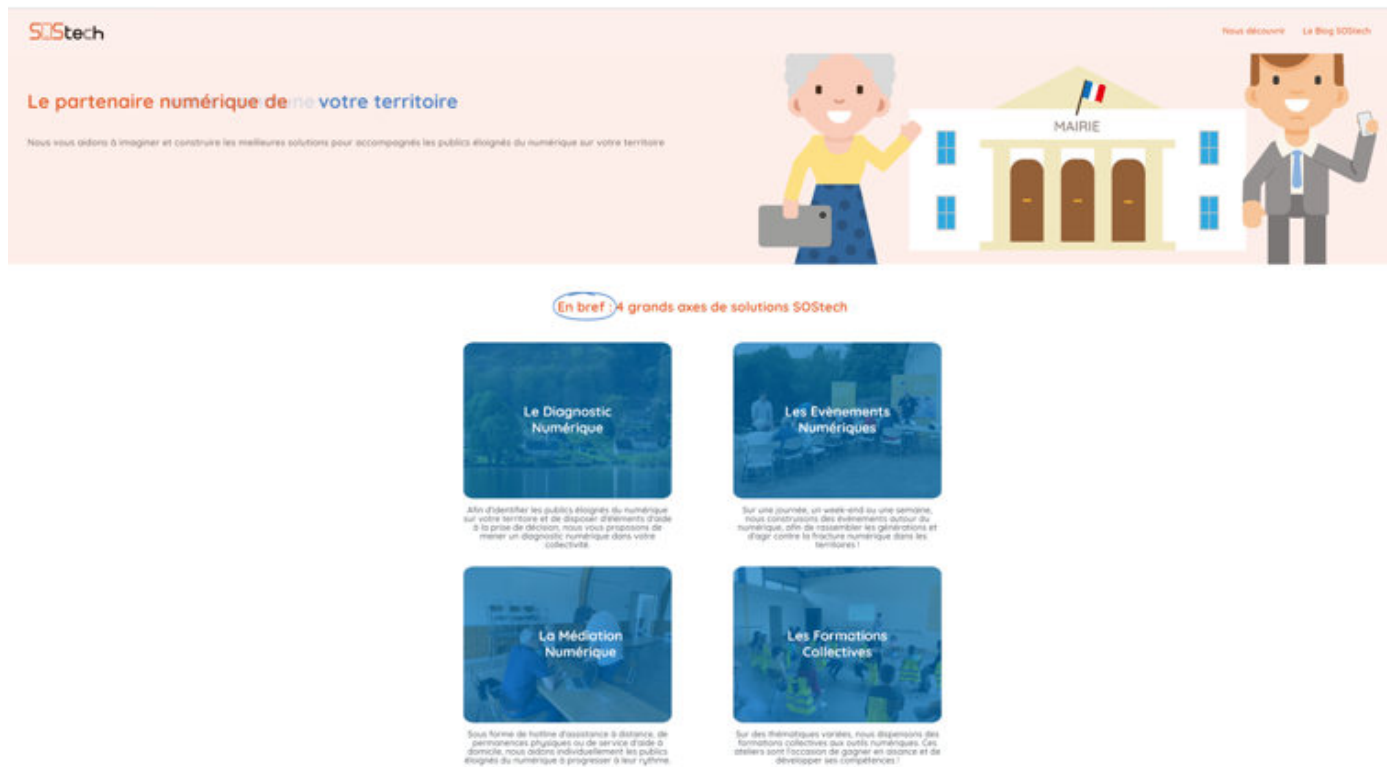


Figure 47 : Site Internet de SOS Tech



2. Discours médiatique et publicitaire

Les discours médiatiques peuvent être modifiés en intégrant les valeurs motivationnelles dominantes (2.1.), en agissant sur une réduction de la distance psychologique avec les violations de données personnelles (2.2.) ou en se basant sur des dynamiques collectives (2.3.).

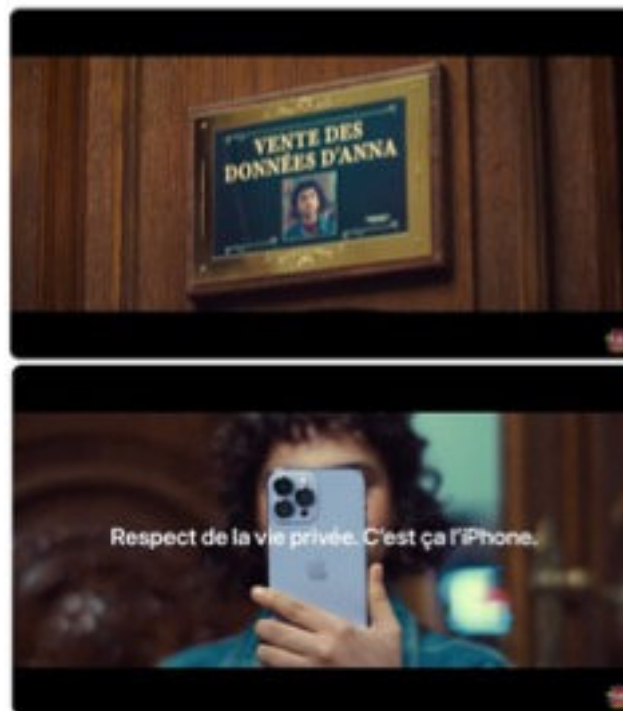
2.1. Discours publicitaires mobilisant les préférences motivationnelles

Notre recherche met en avant trois valeurs motivationnelles dominantes : l'équité sociale et de genre, la liberté et la sécurité. Nous recommandons que les messages publicitaires intègrent principalement ces valeurs et soient plus clairs dans leurs discours.

Pour illustration, nous présentons une publicité Apple (Figure 48), qui ne mentionne aucune des trois valeurs citées et parle de « respect de la vie privée », et une publicité Samsung (Figure 49), qui parle plus clairement de « sécurité ». Mais aucune n'apporte la preuve de sa déclaration.

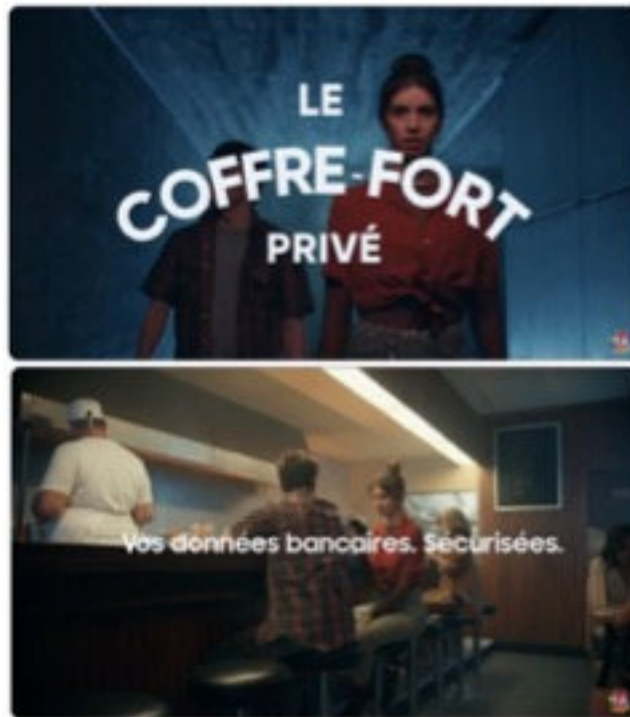
De plus, dans l'essai micro, nous montrons que la préoccupation pour la protection de la vie privée (« respect de la vie privée ») est un facteur psychologique de moindre importance en comparaison avec la distance psychologique avec les violations de données personnelles.

Figure 48 : Exemple de publicité Apple¹³⁴



¹³⁴ Publicité disponible à : <https://www.youtube.com/watch?v=ULEIqIsTpmc>

Figure 49 : Exemple de publicité Samsung¹³⁵



2.2. Réduction de la distance psychologique avec les violations de données personnelles

Comme nous l'avons expliqué page 299 sur la base des travaux de Didi Alaoui & Cova (2021), la distance psychologique est utilisée en marketing pour activer certains leviers et favoriser certains types de réponses du consommateur. Par exemple, Amazon joue sur la distance temporelle en mettant en avant la rapidité de ses livraisons pour activer l'acte d'achat, tandis qu'Hermès, tout en mobilisant aussi la distance temporelle, va mettre en avant un délai long de disponibilité de ses produits pour activer le sentiment de rareté et d'exclusivité d'un sac à main et favoriser l'acte d'achat.

Notre contexte présente un triple challenge : (i) réussir à réduire la distance psychologique avec les violations de données personnelles, en jouant par exemple sur la distance sociale et temporelle (i.e., une violation peut arriver n'importe quand et à n'importe qui), (ii) tout en restant positif et en incitant à l'action. Par exemple, en jouant sur les niveaux de représentation et d'abstraction aboutissant à des évaluations des risques positifs ou négatifs, une représentation abstraite telle que « protéger sa vie privée » pourrait conduire à une évaluation plus positive de

¹³⁵ Publicité disponible à : https://www.youtube.com/watch?v=qV8uf_c1Fe4

cette activité alors qu'une représentation concrète comme « arrêter d'utiliser WhatsApp » ou « n'accepter aucun cookie sur les pages web » pourrait aboutir à une évaluation négative de cette même activité. Enfin (iii) les distances psychologiques ne sont pas les mêmes selon les préférences culturelles et les groupes sociaux : il faut donc adapter les messages.

Pour répondre à ce triple challenge :

- il nous semble que des campagnes de communication sur des messages courts et simples pourraient être efficaces, comme :
 - « **ne pas accepter les Wifi gratuits => restez sur votre 4G/5G** »
 - « **la police vous a envoyé un mail pendant la nuit => ne l'ouvrez pas** »
 - « **vous êtes victime d'un chantage à la webcam** (i.e., on vous menace de diffuser une vidéo intime) => **vous n'êtes pas seule, appelez le 640** » (nota bene : à ma connaissance, il n'existe pas de numéro d'urgence court dans ce cas, ce qui me semble une erreur ; le 640 est fictif) ;
- comme tous les annonceurs le savent, il faut construire une campagne de communication alliant spots télévisés et médias plus locaux comme la radio et l'affichage permettant d'adapter les messages publicitaires aux bassins de population ;
- il faut faire appel à des professionnels pour construire les messages, tant des agences de publicité que des professionnels de la cybersécurité, comme l'ANSSI, qui propose des formations très didactiques (cf. Figure 50 ci-dessous), et ce par des mécanismes d'appels à concours que la CNIL pourrait proposer.

Figure 50 : Message publicitaire des formations de l'ANSII



2.3. Utilisation de dynamiques collectives

Nos résultats indiquent que la protection de la vie privée est « l'affaire de tous », en se basant sur des dynamiques collectives. Nous invitons les acteurs à développer des messages médiatiques et publicitaires dans ce sens. À titre d'exemple, le spot publicitaire de l'ANSII (cf. Figure 51) utilise des expressions telles que « la cybersécurité est l'affaire de tous » ou « face aux risques cyber, vous n'êtes pas seuls », mobilisant donc des ressorts collectifs.

Figure 51 : Exemple de publicité de l'ANSII¹³⁶



Face aux risques cyber
de vraies solutions existent.

cybermalveillance.gouv.fr

¹³⁶ Publicité disponible à : <https://lnkd.in/eU5EcasP>

3. Évolutions réglementaires

Sur la base de nos travaux, nous formulons trois recommandations pour les réglementations :

- La nécessité d'adaptations locales d'un cadre réglementaire plus global ;
- La nécessité de moyens de recours au droit plus collectifs.

Dans un troisième paragraphe, nous discutons également la nécessité de faire coïncider les plaintes pour violations et les déclarations des entreprises.

3.1. Adaptation locale des réglementations internationales

Dans notre essai micro, en identifiant les mécanismes culturels dans la plainte pour violation de la protection des données personnelles, nous avons fourni des recommandations pour des politiques localisées de protection de la vie privée. Nous rappelons quelques grandes lignes. La mise en œuvre des politiques publiques dans une perspective plus large que les politiques nationales, telle que la perspective européenne, doit tenir compte des différences culturelles pour être efficace (Bellman et al., 2004; Milberg et al., 2000) selon l'adage : « *Think global, act local* ». Par ailleurs, tout en insistant sur la nécessité d'harmonisation européenne de la mise en œuvre du RGPD, la Commission européenne recommande d'adapter les moyens de déploiement à l'échelle nationale, afin de modifier le comportement et le mode de pensée de tous les acteurs, avec par exemple « la conception d'outils appropriés et de formats et d'interfaces standard »¹³⁷ (p.10). En d'autres termes, chaque pays avance à son rythme et en coordination avec les autres, l'objectif étant que chacun parvienne au même niveau de protection des données personnelles des citoyens et de déploiement de l'ensemble des outils prévus dans le cadre du RGPD. À titre d'exemple, les pays collectivistes, où les personnes ont tendance à moins se plaindre, devraient renforcer les ressources financières et humaines des autorités de protection des données pour développer les activités de contrôle de la conformité

¹³⁷ Communication de la commission au parlement européen sur la protection des données (disponible le 29 juillet 2022 à : <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0115:FIN:EN:PDF>)

au RGPD¹³⁸, et favoriser les sanctions sur la base d'actions collectives. Cette implication pratique est davantage développée dans le chapitre 4 (essai macro), pages 202 à 203.

3.2. Nécessité de possibilités de plaintes collectives

En montrant que la distance psychologique avec la violation de données personnelles joue un rôle de premier ordre dans la réponse du consommateur face à une violation de données personnelles et que l'égalité socio-genrée est l'orientation culturelle la plus influente, cette recherche fait écho aux travaux de Pasquier (2018) sur l'Internet des familles rurales. Nous mettons en avant le fait que les familles modestes se soucient essentiellement du piratage et de l'usurpation d'identité, mais pas du tout de la protection des données personnelles ou de la souveraineté numérique, et que la conception de la vie privée relève moins de l'individu que du groupe familial. Ces résultats permettent à la CNIL d'éclairer un rapport alternatif aux technologies et à la protection des données personnelles, qui vient enrichir les pistes d'actions des services publics, notamment pour répondre à une exigence de réduction de la fracture numérique et à un impératif de désenclavement face au tout numérique des services publics.

Ce constat d'importance de l'égalité socio-genrée répond également aux appels de plusieurs chercheurs, selon lesquels « il paraît nécessaire de cesser de penser individuellement la vie privée, de cesser de la considérer comme un arbitrage que chacun serait amené à faire. Nous devons plutôt y réfléchir comme un droit collectif, par lequel, même si nous n'avons rien à cacher, il est aussi dans l'intérêt de tous de vivre dans une société où certains (...) puissent avoir des choses à cacher » (Cardon, 2019, p.418). Si la protection des données personnelles est un droit privé, les leviers d'action qui la concernent sont de nature collective.

Enfin, les acteurs sont demandeurs vis-à-vis de la CNIL de pouvoir « monter en collectif » et de faciliter les possibilités de recours collectif à la protection des droits individuels. En effet, comme nos résultats l'ont montré (essai méso), les individus se sentent souvent désarmés ou peu en capacité d'aller porter plainte à la CNIL.

¹³⁸ On note par exemple en 2022 une augmentation du budget de la CNIL et une externalisation du traitement des plaintes (<https://www.dastra.eu/fr/article/la-cnil-va-augmenter-son-budget-en-2022-pour-repondre-au-defi-du-rgpd/47508>)

3.3. Efficacité des moyens de recours au droit en vue d'une indemnisation des victimes

Enfin, nous souhaitons discuter l'efficacité des moyens de recours au droit, le rôle des plaintes (même collectives), et des obligations de déclaration des entreprises, en vue d'interroger une efficacité de déclaration, d'action et d'indemnisation. Car in fine, quel est le moyen efficace pour la protection et le dédommagement des individus ? Nos résultats obtenus à travers l'essai 2 (méso) concernant les plaintes à la CNIL (cf. Tableau 42) soulignent en effet la complexité des procédures de dépôt de plainte (nécessitant compétences juridiques et techniques) et un manque de légitimité et d'efficacité par rapport à une action en justice.

Pour rappel, le RGPD (Art. 33 et 34) impose aux entreprises de signaler toute violation de données en informant la personne dont les données personnelles ont été violées (cf. Annexe 1). Le non-respect de ce principe peut entraîner des amendes (maximum possible de 20 millions d'euros ou 4% du chiffre d'affaires). En théorie, les violations de données personnelles ne sont pas découvertes grâce aux plaintes (efficacité de déclaration) : est-ce la réalité ?

Toute personne a la possibilité de porter plainte auprès de la CNIL si elle souhaite signaler une atteinte aux règles de protection de données personnelles par un organisme. La CNIL peut alors décider de mesures correctrices mais elle ne peut pas obtenir des dommages et intérêts pour le plaignant¹³⁹. De plus, les associations de défense des droits et des libertés qui déposent régulièrement des plaintes à la CNIL « ont parfois l'impression que l'organisme mis en cause reçoit plus d'informations que le plaignant. » (rapport Atelier CNIL, page 3¹⁴⁰). Par conséquent, tout signalement de violations de données personnelles semble avoir pour conséquence une pression sur l'entreprise pour modifier ses pratiques, ce qui est déjà bénéfique pour les individus et consommateurs (efficacité d'action).

En revanche, ces signalements ne semblent avoir aucun intérêt direct pour les individus et consommateurs en vue d'une indemnisation (efficacité d'indemnisation), et c'est pourquoi des collectifs lancent des actions en justice et des recours en Conseil d'État. Il nous semble qu'une réflexion doit absolument être envisagée sur ce point.

¹³⁹ <https://www.cnil.fr/fr/adresser-une-plainte>

¹⁴⁰ Rapport « Atelier CNIL Associations de défense des droits et libertés, partenariat pour un gouvernement ouvert » disponible à : <https://www.cnil.fr/fr/faire-dun-droit-individuel-un-sujet-collectif-rencontres-entre-la-societe-civile-et-la-cnil-autour>

Section 3. Limites et voies de recherche

Pour finir, notre recherche a plusieurs limites conceptuelles : (i) identifiées au regard des recherches actuelles, (ii) ou points qui pourraient être approfondis dans la continuité de nos travaux. Nous synthétisons ces limites dans le Tableau 59 page suivante, puis nous les détaillons autour de 3 axes de recherche : vie privée (1.), réponses aux violations de données personnelles (2.), culture et vie privée (3.). Ces limites constituent autant de voies de recherches (également précisées dans le Tableau 59) qui pourraient être conduites à l'issue de cette thèse de doctorat, celle-ci devant aboutir au lancement d'une carrière académique. Il s'agit des limites globales de notre thèse : certaines limites plus spécifiques (notamment méthodologiques) sont reprises à la fin de chaque essai (macro, méso, micro).

1. Protection des données personnelles et de la vie privée

1.1. Compréhension théorique de la pratique

La première limite que nous identifions réside dans la compréhension de la pratique sociale de la protection de la vie privée. En effet, dans notre essai méso, notre approche à travers des entretiens semi-directifs reste centrée sur l'individu (agent) et moins sur la pratique sociale en elle-même (Bourdieu, 1972). Nous avons expliqué page 242 que d'autres études s'appuyant sur la théorie de la pratique reposent également essentiellement sur des entretiens : par exemple, dans la compréhension du développement de la marche nordique (Shove & Pantzar, 2005) ou dans l'exploration des pratiques de consommation d'alcool chez les adolescentes australiennes (Lunnay et al., 2011). De plus, l'approche de Giddens (1984) fonde sa théorie sur l'idée que l'action individuelle est représentative de la structure sociale.

Cependant il nous semble que notre recherche gagnerait en consistance et en compréhension en étant complétée par des informations dans un objectif de triangulation des données : par exemple avec un journal de bord d'une personne engagée dans la protection de la vie privée. De plus, il serait intéressant d'observer la pratique inverse, i.e., de non-engagement dans la protection de la vie privée, afin d'identifier les structures qui conduisent les individus à être enfermés dans des pratiques de divulgation de leurs données.

Tableau 59 : Limites et voies de recherche

	Limites	Voies de recherche
Vie privée	- Approfondissement de la compréhension théorique de la pratique de la vie privée	- Compléter avec des données illustratives des pratiques (e.g., journal de bord)
	- Compréhension de la distance psychologique avec les violations de données personnelles	- Développer une échelle de distance psychologique avec les violations de données - Approfondir le lien entre dimensions de la distance psychologique et de la culture
	- Approfondissement du lien entre vie privée et cybersécurité	- Explorer le comportement du consommateur en situation de vulnérabilité informatique
Réponses face à une violation de données personnelles	- Définition des violations de données par les consommateurs	- Identifier les critères permettant à un utilisateur de définir une violation de données personnelles
	- Lien entre préjudices, réponses et dédommagement des consommateurs	- Comprendre les attentes des consommateurs en termes de dédommagements en cas de violations de données personnelles
	- Lien entre violations de données personnelles et pratiques de publicité digitale	- Intégrer une politique de cybersécurité dans les stratégies publicitaires et marketing des entreprises
Culture et vie privée	- Compréhension des effets culturels sur la protection de la vie privée dans des pays émergents (notamment effets d'une préférence pour le collectivisme)	- Faire des recherches empiriques dans des pays émergents (BRICS)
	- Approfondissement des mécanismes d'influence culturelle (variable médiatrice, modératrice, etc.)	
	- Application aux problématiques de transferts internationaux de données	

1.2. Compréhension théorique de la distance psychologique

Comme nous l'avons indiqué dans notre essai micro (cf. page 320), il n'existe pas d'échelle validée ni pour la mesure de la distance psychologique avec la vie privée (Bandara et al., 2021), ni pour la mesure de la distance psychologique avec les violations de données personnelles. Pour cette raison, nous avons utilisé plusieurs sources pour construire nos items (Spence et al., 2012 ; Bandara et al., 2018). Entre-temps, Bandara et al. (2021) ont proposé une échelle de distance psychologique avec la vie privée. Or, comme nous avons montré que la distance psychologique avec les violations de données avait un rôle plus important que le souci de contrôle de ses données personnelles dans les mécanismes psychologiques reliant culture et réponses, il serait intéressant d'approfondir une échelle de distance psychologique avec les violations de données personnelles.

De plus, une exploration en profondeur des différentes dimensions de la distance psychologique s'impose : (i) dans le lien entre orientations culturelles et dimensions de la distance psychologique (e.g., lien entre distance sociale et relation à l'*endogroupe* et à l'*exogroupe*), (ii) dans le lien entre dimensions de la distance psychologique et types de réponses (e.g., quel impact de la distance hypothétique sur les différents types de réponses ?), (iii) et dans la significativité des dimensions (e.g., distance temporelle non significative ?).

1.3. Approfondissement du lien entre vie privée et cybersécurité

En introduction, nous avons affirmé vouloir inscrire notre recherche en vie privée, faisant écho à de récents travaux explorant les questions de perte de contrôle et donc de vulnérabilité des individus (e.g., Del Bucchia et al., 2021) dans un contexte de digitalisation accrue de nos économies, de risques croissants de sécurité informatique et de violations de données personnelles (Rasoulouian et al., 2021). Notre objectif est de développer une meilleure compréhension de la vulnérabilité du consommateur en situation d'insécurité informatique. Ceci permettrait de répondre à de nombreux experts en cybersécurité (e.g., Arpagian, 2022 ; Weber & Jean-Philippe, 2017), appelant à développer une culture de la cybersécurité dans nos sociétés pour que les consommateurs deviennent technologiquement responsables. Nous avons alors évoqué la possibilité que notre recherche puisse adopter un positionnement en sociologie de la cybersécurité, similaire à ce que la sociologie de la santé est à la médecine, et visant donc

à mieux comprendre les interactions entre la société (et les individus qui la composent) et les risques liés à la sécurité informatique (portant notamment sur la perte de vie privée), afin de proposer des pratiques et actions pour soutenir le développement d'une cybersécurité efficace. Nous espérons à travers notre recherche avoir ouvert de nouvelles voies de recherche, à approfondir par la suite.

2. Réponses apportées aux violations de données personnelles

2.1. Définitions des violations de données personnelles en marketing

Dès notre introduction (page 6), nous avons défini une violation de données personnelles comme étant un vol intentionnel d'informations confidentielles, touchant des individus, dans un objectif lucratif. Nous avons rappelé la définition inscrite au RGPD, et exposé les critères pris en compte dans les recherches en sécurité informatique (e.g., intentionnalité, gravité) pour définir une violation de données. Nous avons souligné qu'à date, les recherches en marketing proposent de définir les violations de données personnelles comme des défaillances de service (Rasoulouian et al., 2021).

Par ailleurs, nous avons observé, dans notre essai méso, que la perception d'un comportement engagé pour la protection de la vie privée était très subjective et variable. Dans notre essai micro, certaines questions concernant principalement les contextes et les types de violation de données personnelles demeurent. Par exemple, nous avons testé deux scénarios de violations de données : piratage de l'accès à un site Internet et piratage d'une carte de crédit. De nouveaux tests avec d'autres scénarios de violation, au regard du fait que près de deux tiers de nos répondants ont déjà été victimes d'une violation de données, principalement liées à l'usage des outils informatiques, apporteraient plus de matière au sujet.

C'est pourquoi il nous semble important d'initier une recherche permettant d'identifier les critères permettant à un utilisateur de définir une violation de données personnelles.

2.2. Lien entre préjudice, réponses et dédommagement

Notre recherche visait à comprendre les réponses face aux violations de données personnelles, dans un objectif d'identifier des pistes permettant de mieux protéger les consommateurs en situation de vulnérabilité informatique. Dans ce même cadre, et pour permettre une bonne interprétation juridique des préjudices liés à une violation de données personnelles, évitant ainsi que celles-ci ne donnent lieu à aucune réparation faute de préjudice identifiable, Citron et Solove (2021) ont proposé une typologie des préjudices (cf. Tableau 6). Malgré cela, les recours en justice restent peu instruits (Citron & Solove, 2021; Romanosky et al., 2013) et les consommateurs très faiblement indemnisés. Enfin, dans cet objectif, les associations de consommateurs tardent selon nous à s'emparer du sujet : à titre d'exemple (cf. page 233), malgré de nombreuses et insistantes tentatives, nous n'avons pas réussi à obtenir des entretiens avec des associations françaises de protection des consommateurs (UFC Que Choisir et 60 millions de consommateurs). Au moment où nous finalisons la rédaction de ce manuscrit, l'association UFC Que Choisir lance fin janvier 2023 la campagne « je ne suis pas une data »¹⁴¹ et la plateforme « respectemesdatas.fr »¹⁴².

Par ailleurs, de nombreux travaux en marketing illustrent le poids des dédommagements dans les relations avec les clients après une rupture de service (Gelbrich et al., 2015, 2016; Grégoire & Fisher, 2008). Dans cet objectif, il nous paraît important de compléter les travaux de Citron et Solove (2021) et d'établir le lien entre préjudice, réponses et dédommagement perçu par les consommateurs (d'un point de vue marketing et non juridique).

Enfin, plusieurs questions se posent qu'il serait intéressant de continuer à explorer :

- Dans un contexte d'insécurité informatique qui touche les différentes parties prenantes, les violations de données personnelles doivent-elles être comprises comme des ruptures de service ? Par là même, qui porte la responsabilité de la violation de données ?
- A quel degré évaluer l'insatisfaction du client, alors que le souhait de vengeance (lié un sentiment de trahison fort suite à la rupture du contrat social de protection des données personnelles ; Grégoire et al., 2009) ne peut pas forcément s'exprimer ?
- Enfin existe-t-il de nouvelles formes d'expression de l'insatisfaction (ou de la vengeance) comme la résistance aux nouvelles technologies (Chamaret et al., 2020) ?

¹⁴¹ <https://www.jenesuispasunedata.fr/>

¹⁴² <https://www.respectemesdatas.fr/>

2.3. Violations de données dans un contexte de publicité digitale

Nous avons exclu de notre recherche les violations de données personnelles dans un contexte de publicité digitale. Or, il existe actuellement un débat ardent sur la légalité des pratiques de la publicité digitale (e.g., publicité programmatique, système d'enchères, analyse de trafic web), qui repose principalement sur l'exploitation de données personnelles fournies par les cookies tiers. Le RGPD a imposé certaines règles (e.g., consentement obligatoire) et interdit les cookies tiers. Cette interdiction des cookies tiers a souvent été reportée pour éviter de déstabiliser le marché publicitaire mondial. Également, en janvier 2022, l'autorité autrichienne de protection des données personnelles a jugé l'utilisation de Google Analytics contraire au RGPD¹⁴³ et a été suivie par ses homologues européens. De plus, l'Irish Council for Civil Liberties a dévoilé en mai 2022 que des informations de géolocalisation ou d'historique de navigation sont collectées et revendues à des data brokers, assimilant ainsi certaines pratiques de publicité programmatique à « la plus grande fuite des données »¹⁴⁴.

Ce constat soulève plusieurs questions :

- Est-ce que les consommateurs perçoivent les pratiques de publicité digitale comme des violations de données personnelles ? (point à intégrer dans les définitions de violations personnelles évoquées en 2.1).
- Quel est l'impact de ces pratiques publicitaires et des violations de données personnelles sur la politique marketing des entreprises ?

Ces questions sont lourdes d'impact dans les stratégies marketing et publicitaires des entreprises, mais également dans les choix organisationnels des entreprises. Elles nécessiteraient d'être plus explorées.

¹⁴³ https://www.lemonde.fr/pixels/article/2022/01/20/l-utilisation-de-google-analytics-jugee-contraire-au-droit-europeen-sur-les-donnees-personnelles_6110287_4408996.html

¹⁴⁴ Le Monde (16.05.2022) : Publicité programmatique : les données personnelles des internautes diffusées à leur insu plusieurs centaines de fois par jour (accessible à : <https://www.lemonde.fr/pixels/article/2022/05/16/publicite-programmatique-les-donnees-personnelles-des-internautes-diffusees-a-leur-insu-plusieurs-centaines-de-fois-par-jour>)

3. Culture et souci de protection de la vie privée

3.1. Compréhension des effets culturels sur la protection de la vie privée dans des pays émergents

Notre recherche a exploré l'influence de la culture sur les réponses aux violations de données personnelles, dans le cas de l'Europe et de la France. Nos résultats, obtenus dans le cadre hexagonal, permettent de comprendre la variabilité au niveau international dans le nombre de plaintes notifiées pour violations de données personnelles, notamment entre pays européens.

Nous pensons qu'ils apportent une base intéressante pour mieux comprendre les effets culturels sur la protection de la vie privée dans les pays émergents (e.g., Nigéria, Afrique du Sud) et les BRICS (e.g., Brésil, Chine, Inde), qui restent ignorés par la recherche sur les données personnelles malgré de nombreuses réglementations, des échanges internationaux de données personnelles et des principes d'extraterritorialité de nos réglementations. Certains phénomènes restent obscurs, comme le surprenant refus de l'Inde en 2016 de l'offre d'Internet gratuit Free Basics de Facebook (avec des manifestations citoyennes importantes pour défendre la neutralité du web). De plus, les motivations à établir ces réglementations ne sont pas toujours évidentes : par exemple, le Maroc a mis en place dès 2009 un régulateur (CNDP, Commission Nationale de Contrôle de la protection des données à caractère personnel) pour pouvoir maintenir des activités d'off-shorings avec ses voisins européens. C'est pourquoi Martin & Murphy (2017) ont appelé l'exploration nécessaire de phénomènes de protection de la vie privée dans les pays émergents.

L'exploration des pays émergents nécessite une certaine vigilance. S'ils se ressemblent selon certains critères (e.g., recherche d'indépendance, post-colonialisme, fort sentiment national, fort développement économique, fort sentiment de sécurité intérieure), ils diffèrent de par leurs histoires, constructions, religions et régimes politiques.

3.2. Application aux problématiques de transferts internationaux de données

Comme nous l'avons déjà mentionné, les questions de transferts internationaux de données personnelles font l'objet de nombreux débats voire conflits, principalement entre l'Europe et les États-Unis, suite à l'invalidation du Privacy Shield, mais également récemment entre l'Europe et la Chine avec l'interdiction de l'usage de Tik Tok. Ces questions sont parfois « l'arbre qui cache la montagne » de conflits économiques plus ardents (e.g., revenus publicitaires générés par Tik Tok qui échappent au marché européen). Cependant dans la continuité de nos travaux, il nous semble que des aspects pourraient être approfondis sur les équivalences culturelles et/ou contextuelles des fondements des diverses réglementations internationales.

Conclusion générale

Dans cette recherche, nous explorons l'influence d'effets culturels sur les réponses face aux violations de données personnelles, à différents niveaux d'observation (macro, méso, micro). Ceci nous permet d'identifier plusieurs phénomènes non encore observés.

Premièrement, nous montrons que le souci de défense d'une **équité sociale et de genre** amène les individus à adopter des réponses plus actives face à une violation de leurs données personnelles. Nous identifions deux autres motivations culturelles : **liberté et sécurité**. Nous apportons alors des éclairages culturels nouveaux dans la compréhension des valeurs fondatrices de la préoccupation pour la protection de la vie privée, remettant en question l'importance d'une préférence à l'individualisme.

Deuxièmement, nous actualisons la compréhension des réponses apportées face aux violations de données personnelles et identifions un type de réponse particulier : la plainte auprès des régulateurs. Cette perspective nous amène à interroger l'**efficacité des réponses et des moyens de recours au droit protégeant l'individu en situation de vulnérabilité informatique**. Nous soulignons que (i) les moyens d'action sont plus efficaces si collectifs, (ii) la perte de contrôle des données peut être pondérée par plus de sécurité.

Troisièmement, nous identifions de nouveaux mécanismes sociologique et psychologique, permettant de mieux comprendre le lien entre culture et réponses. Nous envisageons la **protection de la vie privée comme une pratique sociale**, et non individuelle. Nous montrons également que la **distance psychologique** avec les violations de données personnelles influence plus significativement les réponses que la préoccupation pour la protection de la vie privée.

Par conséquent, l'éclairage de ces phénomènes apporte une compréhension théorique différente de la préoccupation pour la protection de la vie privée. D'une part, la protection de la vie privée est envisagée comme un « mieux vivre ensemble » et non un « mieux vivre tout seul » (importance d'équité sociale) développée autour de pratiques sociales et d'un partage de responsabilités entre acteurs. D'autre part, elle repose sur une préoccupation de « sécurité » et non de « contrôle » (préférence de sécurité, perte de contrôle, priorité donnée à la distance psychologique). Le souci de protection de la vie privée n'est donc pas un souci de contrôler ses données personnelles mais un **souci de sécuriser les données personnelles de tous**.

Cette nouvelle compréhension ouvre des portes théoriques importantes dans le champ des recherches en vie privée, répondant à des appels à de plus amples explorations anthropologiques et culturelles de la vie privée, permettant d'optimiser les approches réglementaires en la matière (e.g., Dinev, 2014; Martin & Murphy, 2017). Ces approches pourraient reposer sur des notions de collectifs (et non une surresponsabilisation individuelle), de sécurité (face à la perte de contrôle de ses données personnelles), de responsabilités développées autour de pratiques à un niveau méso (et non uniquement un cadre réglementaire macro). Ces pistes de réflexion théorique amènent à (i) développer les recherches faisant le lien entre vie privée et sécurité, (ii) interroger le statut des violations de données personnelles (considérées à ce jour comme des ruptures de service).

Ces éléments théoriques sont la base de contributions pratiques, qui s'inscrivent dans un cadre plus général de développement de pratiques de protection de la vie privée à un niveau méso, autour de notions de **responsabilité et de sécurité**. Chaque acteur (e.g., entreprises, structures éducatives, collectivités) doit œuvrer dans ce sens. Les médias et les publicitaires doivent accentuer les messages autour des notions de collectivité, de sécurité et de réduction de la distance psychologique avec les risques de violations de données personnelles. Enfin les réglementations peuvent être améliorées : en s'adaptant localement, en favorisant les plaintes collectives, en facilitant les possibilités de demandes d'indemnisations. Ces propositions répondent ainsi aux appels des acteurs de la cybersécurité qui souhaitent diffuser une culture de sécurité informatique pour développer des pratiques technologiques responsables chez les consommateurs.

En bref, équité, liberté, sécurité : la protection du consommateur en situation de vulnérabilité informatique repose sur un souci de sécuriser les données personnelles de tous !



Liste des tableaux

Tableau 1 : État des recherches.....	4
Tableau 2 : Données personnelles objectives et subjectives (Rochelandet, 2010).....	21
Tableau 3 : Législations internationales en matière de protection de données personnelles et degrés de conformité avec le RGPD.....	45
Tableau 4 : Classification des violations de données selon leurs causes et points d'accès (Khan et al., 2021)	53
Tableau 5 : Impact des violations sur les données personnelles (Khan et al., 2021).....	54
Tableau 6 : Typologie de préjudices de violations de données personnelles (Citron & Solove, 2021)	57
Tableau 7 : État des recherches portant sur les violations de données personnelles	60
Tableau 8 : Recherches interculturelles sur la vie privée comparant des pays.....	66
Tableau 9 : Recherches en cross-cultural privacy utilisant d'autres modèles qu'Hofstede.....	67
Tableau 10 : Définitions des 6 dimensions d'Hofstede.....	69
Tableau 11 : Nombre d'occurrences des dimensions d'Hofstede dans les recherches mobilisant le modèle.....	70
Tableau 12 : Recherches mobilisant le modèle d'Hofstede sans identifier d'effets spécifiques des dimensions culturelles	71
Tableau 13 : Recherches mobilisant le modèle d'Hofstede montrant un souci de protection de la vie privée plus important dans les pays individualistes	72
Tableau 14 : Recherches mobilisant le modèle d'Hofstede montrant un souci de protection de la vie privée moins important dans les pays individualistes	73
Tableau 15 : État des recherches portant sur l'influence de la culture sur le souci de contrôle de ses données personnelles.....	75
Tableau 16 : Différentes définitions de la vie privée (Martin & Murphy, 2017)	90
Tableau 17 : Conceptualisation et échelles en matière de protection de la vie privée.....	92
Tableau 18 : Trois niveaux d'observation de la privacy (Martin & Murphy, 2017).....	102
Tableau 19 : Facteurs influençant le souci de vie privée (Li, 2012).....	110
Tableau 20 : Individualisme et collectivisme vertical et horizontal de Triandis (1996)	143
Tableau 21 : Exemples de valeurs terminales et instrumentales (Rokeach, 1973).....	145
Tableau 22 : 10 types motivationnels de Schwartz et les valeurs simples correspondants (Schwartz, 2006)	147
Tableau 23 : Comparaison des dimensions culturelles d'Hofstede et de Schwartz (De Mooij, 2017)	150
Tableau 24 : Synthèse des fondements théoriques de la thèse.....	160
Tableau 25 : Cadres théoriques utilisés dans la thèse	166
Tableau 26 : Hypothèses métathéoriques et paradigmes de recherche (Weber, 2004)	168
Tableau 27 : Détails des collectes de données réalisées dans chaque essai.....	172
Tableau 28 : Apports de chaque essai à la thèse	176
Tableau 29 : Contributions des auteurs et état d'avancement de chaque publication	177
Tableau 30 : Statistiques descriptives et corrélations des dimensions d'Hofstede sur 27 pays européens	191
Tableau 31 : Analyse factorielle des dimensions d'Hofstede sur 27 pays européens	192
Tableau 32 : Nombre de plaintes et dimensions culturelles pour 25 pays européens.....	198
Tableau 33 : Résultats de la première régression.....	199
Tableau 34 : Résultats de la deuxième régression pour les 4 périodes	201
Tableau 35 : La théorie de la pratique	222
Tableau 36 : Profils des personnes interrogées.....	235
Tableau 37 : Tableau comparatif des méthodes.....	241

Tableau 38 : Détail des réponses techniques	249
Tableau 39 : Avantages et inconvénients des réponses techniques possibles	250
Tableau 40 : Illustrations des actions sociales	253
Tableau 41 : Illustrations des réponses sociales	254
Tableau 42 : Avantages et inconvénients des actions conduites auprès de la CNIL	257
Tableau 43 : Éléments du chaînage cognitif	260
Tableau 44 : Verbatims illustratifs des conséquences	261
Tableau 45 : Verbatims illustratifs des valeurs	262
Tableau 46 : Formes de compétences individuelles	279
Tableau 47 : Formes de compétences collectives	281
Tableau 48 : Dimensions de la distance psychologique et applications dans un contexte de consommation (Didi Alaoui & Cova 2021)	300
Tableau 49 : Distance psychologique et préoccupations pour la protection de la vie privée	302
Tableau 50 : Définitions des orientations culturelles de Sharma (2010)	307
Tableau 51 : Indices de validité réelle et de convergence	321
Tableau 52 : Typologie de réponses face à une violation de données personnelles	323
Tableau 53 : Mesure des corrélations des mesures entre les scénario 1 et 2	328
Tableau 54 : Résultats pour le scénario 1 (cas de piratage de ses accès à un site Internet) ...	331
Tableau 55 : Résultats pour le scénario 2 (cas de piratage de sa carte de crédit bancaire)....	332
Tableau 56 : Principaux résultats de chaque essai	343
Tableau 57 : Principales valeurs culturelles identifiées	346
Tableau 58 : Acteurs de la pratique sociale de la protection de la vie privée	368
Tableau 59 : Limites et voies de recherche	381

Liste des figures

Figure 1 : Définition des violations de données personnelles.....	6
Figure 2 : Classification des types, accès et utilisations de données personnelles	24
Figure 3 : Principales étapes de l'histoire de la protection de la vie privée	39
Figure 4 : Carte des législations internationales de protection de données personnelles	44
Figure 5 : Valeur totale des amendes imposées dans le cadre du RGPD par chaque autorité nationale de protection des données personnelles (en € entre le 25 mai 2018 et le 27 janvier 2023)	48
Figure 6 : Exemples de valeurs de dimensions d'Hofstede pour quelques pays européens.....	68
Figure 7 : Champs académiques des fondements théoriques de la thèse.....	82
Figure 8 : Pyramide des degrés de vulnérabilité (Martin, Borah & Palmatier, 2017)	96
Figure 9 : État de la littérature en matière de protection de la vie privée du consommateur (Beke et al., 2018).....	103
Figure 10 : Théories mobilisées dans les recherches en préoccupation pour la protection de la vie privée (Li, 2012)	106
Figure 11 : Processus de réponse à une attente non satisfaite.....	115
Figure 12 : Réponses pour la protection de la vie privée (Son & Kim, 2008).....	122
Figure 13 : Réponses face à une violation de données personnelles	124
Figure 14 : Influence de facteurs contextuels sur le comportement individuel (Matsumoto, 2007)	131
Figure 15 : Différents niveaux de culture (Prime & Usunier, 2012)	132
Figure 16 : Trois blocs composant la culture (adapté de Schein et al. (2015), Trompenaars (1996) et Hout (1969)).....	133
Figure 17 : Rôle des valeurs dans les processus de socialisation (Ladwein, 2003).....	137
Figure 18 : Chronologie des contributions majeures à la théorie des dimensions culturelles	141
Figure 19 : Système initial de valeurs de Schwartz	146
Figure 20 : Nouveau système des 19 valeurs de Schwartz (Schwartz et al., 2012).....	148
Figure 21 : Niveaux institutionnel, interpersonnel et individuel	154
Figure 22 : Trois niveaux d'observation de l'influence de la culture	164
Figure 23 : Modèle conceptuel de la thèse.....	166
Figure 24 : Processus de collecte de données	171
Figure 25 : Cadre conceptuel de l'essai 1 portant sur l'influence de la culture nationale.....	196
Figure 26 : Représentation des 23 pays européens selon leur nombre de plaintes et les facteurs d'individualisme et de masculinité.....	204
Figure 27 : Réponses face à une violation de données personnelles	220
Figure 28 : Structure sociale et habitus de Bourdieu (Catinaud, 2015)	223
Figure 29 : Structure de la théorie de la pratique de Giddens.....	224
Figure 30 : Schéma conceptuel de l'essai.....	230
Figure 31 : Étapes de la méthodologie.....	231
Figure 32 : Schéma général de présentation des résultats.....	242
Figure 33 : Actions de protection des données personnelles	246
Figure 34 : Schéma motivationnel pour des valeurs d'équité	266
Figure 35 : Schéma motivationnel pour des valeurs de liberté.....	268
Figure 36 : Schéma motivationnel pour des valeurs d'individualité.....	270
Figure 37 : Structure de pratique sociale de protection de la vie privée.....	272
Figure 38 : Typologie de réponses face à une violation de données personnelles	295
Figure 39 : Modèle conceptuel de l'essai 3 niveau Micro.....	319
Figure 40 : Résultats obtenus avec le scénario 1	331

Figure 41 : Résultats pour le scénario 2.....	332
Figure 42 : Apports théoriques et pratiques des résultats de la recherche	345
Figure 43 : Proposition de définition pour la protection de la vie privée	361
Figure 44 : Structure de la pratique sociale de la protection de la vie privée	363
Figure 45 : Applications pratiques des éléments de la structure de la pratique sociale.....	364
Figure 46 : Exemple de Google Classroom	371
Figure 47 : Site Internet de SOS Tech	371
Figure 48 : Exemple de publicité Apple	372
Figure 49 : Exemple de publicité Samsung	373
Figure 50 : Message publicitaire des formations de l'ANSII.....	375
Figure 51 : Exemple de publicité de l'ANSII.....	376

Tables des annexes

Annexe 1 : Exemple de notification de violations de données personnelles	426
Annexe 2 : Ensemble des recherches interculturelles en vie privée	427
Annexe 3 : Ensemble des Data Protection Authorities (DPA) en Europe	429
Annexe 4 : Principales théories mobilisées dans les recherches en vie privée (Li, 2012).....	431
Annexe 5 : Autorités européennes compétentes dans le traitement de plaintes pour violations de données personnelles.....	433
Annexe 6 : Modalités de dépôt de plainte sur le site Internet du DPA irlandais	434
Annexe 7 : Scores des dimensions d'Hofstede pour les pays européens.....	435
Annexe 8 : Formulaire de pré-entretien de l'essai 2 niveau Méso	436
Annexe 9 : Guide d'entretien de l'essai 2 niveau Méso.....	438
Annexe 10 : Principaux résultats d'une recherche sur les motifs de recours au droit menée par la CNIL	439
Annexe 11 : Matrice d'implication de l'essai 2 niveau Méso	441
Annexe 12 : Carte hiérarchique de l'essai 2 niveau Méso	441
Annexe 13 : Structure du questionnaire de l'essai 3 niveau Micro	442
Annexe 14 : Caractéristiques de l'échantillon interrogé dans l'essai 3 niveau Micro	443

Tables des matières

Introduction générale	1
Chapitre 1. Contexte général de la recherche	18
Section 1. Contexte managérial de la recherche	19
1. Violations de données personnelles : le « far-west »	19
1.1. Définition et classification des données personnelles	19
1.1.1. Définition des données personnelles	19
1.1.2. Classification des données personnelles	20
1.1.3. Utilisation des données personnelles	23
1.2. Définition des violations de données personnelles	25
1.3. Diversité des violations de données personnelles	27
1.3.1. Scandales emblématiques de violations de données sensibles	27
1.3.2. Cyberattaques des établissements de santé et hospitaliers	28
1.3.3. Exemples historiques de violations de données bancaires ou financières	29
1.3.4. Principales victimes des violations de données : les consommateurs	30
1.4. Volume, tendances haussières et impacts financiers des violations de données personnelles	30
1.5. Cybercriminalité et moyens mis en œuvre face aux violations de données personnelles : le « far-west »	32
1.6. Cybersécurité, sécurité informatique et protection des données personnelles	33
2. Réglementations pour la protection des données personnelles	35
2.1. Histoire de la protection de la vie privée	35
2.1.1. Définition d'un droit fondamental universel à la vie privée	35
2.1.2. Développement de la protection de la vie privée dans les années 1980	37
2.1.3. Mise en place de réglementations spécifiques dans les années 1990	37
2.1.4. Développement des réglementations pour la protection des données personnelles dans les années 2000	38
2.2. Règlement Général pour la Protection des Données personnelles	40
2.2.1. Principes du RGPD	40
2.2.2. Obligations et possibilités instaurées par le RGPD en cas de violations de données personnelles	41
2.2.3. Effets du RGPD sur les pratiques et les violations de données	42
2.3. Réglementations internationales pour la protection des données personnelles en vigueur 43	43
2.4. Variabilité dans la mise en œuvre des réglementations pour la protection des données personnelles	46
2.4.1. Variabilité internationale dans l'interprétation du droit à la vie privée	46
2.4.2. Variabilité entre pays européens dans l'adoption du RGPD	47
Section 2. Contexte académique de la recherche	51
1. Causes et effets des violations de données personnelles	51
1.1. Définitions académiques des violations de données personnelles	51
1.2. Causes et conséquences des violations de données personnelles	52
1.2.1. Causes techniques des violations de données personnelles	52
1.2.2. Conséquences techniques des violations de données personnelles	54
1.3. Conséquences financières pour les entreprises	55
1.4. Conséquences des violations pour les individus et réponses apportées	56
1.4.1. Préjudices des violations pour les individus et citoyens	56
1.4.2. Conséquences psychologiques des violations des données personnelles	58
1.2.3. Réponses des individus face aux violations de données personnelles	59
2. Culture et souci de contrôle des données personnelles	61
2.1. Définition du souci de contrôle des données personnelles	61
2.2. Recherches interculturelles sur la protection des données personnelles	62

2.2.1.	Identification des recherches interculturelles portant sur la protection de la vie privée	62
2.2.2.	Classification des recherches interculturelles portant sur la protection de la vie privée	63
2.2.3.	Recherche séminale d'Altman (1977)	64
2.2.4.	Recherches comparant des pays	65
2.2.5.	Recherches utilisant d'autres modèles que celui d'Hofstede	67
2.3.	Recherches mobilisant le modèle de la culture nationale d'Hofstede	68
2.3.1.	Présentation du modèle de la culture nationale d'Hofstede	68
2.3.2.	Recherches concentrées sur la dimension d'individualisme	70
2.4.	Conclusion des recherches interculturelles sur le souci de contrôle de ses données personnelles	74
2.4.1.	Résultats observés	74
2.4.2.	Appels à de plus amples recherches	76
Section 3.	Axes de recherche et contributions attendues	78
Chapitre 2.	Fondements théoriques	86
Section 1.	Protection des données personnelles	87
1.	Conceptualisation de la protection de la vie privée	87
1.1.	Émergence de la protection de la vie privée dans le champ académique	87
1.2.	Définitions et conceptualisations de la protection des données personnelles	90
1.2.1.	Définitions différentes selon les disciplines et les périodes	90
1.2.2.	Concept basé sur le contrôle et l'auto-gestion de ses données personnelles	91
1.2.3.	Conceptualisations différentes et changeantes	92
1.2.4.	Concept considéré de plus en plus comme abstrait	93
1.2.5.	Traduction française d'information privacy concern	94
1.3.	Dimensions de la préoccupation pour la protection de la vie privée	95
1.3.1.	Contrôle et transparence	95
1.3.2.	Confiance et vulnérabilité	95
1.4.	Dépendance au contexte qui appelle une reconceptualisation	97
2.	Psychologie de la préoccupation pour la protection de la vie privée	101
2.1.	Trois niveaux d'observation (économique, sociétal et psychologique) de la protection de la vie privée	101
2.2.	Cadre général de la psychologie de la vie privée	104
2.2.1.	Modèle APCO	104
2.2.2.	Grandes théories en psychologie de la vie privée	106
2.2.3.	Voies de recherche théorique	107
3.	Autres facteurs influençant les comportements de protection des données ...	109
3.1.	Rôle de la pression sociale	109
3.1.1.	Bénéfices sociétaux	109
3.1.2.	Normes subjectives	109
3.2.	Auto-efficacité	111
Section 2.	Réponses des consommateurs insatisfaits	113
1.	Comportement de plainte du consommateur	114
1.1.	Étapes du processus de comportement de plainte du consommateur	114
1.2.	Étapes du processus de comportement de plainte du consommateur	115
1.2.1.	Étape 1 de la plainte : l'évaluation négative d'une situation	115
1.2.2.	Étape 2 de la plainte : l'appréciation cognitive de la situation	116
1.2.3.	Étape 3 de la plainte : les stratégies d'adaptation et de réponse	116
1.3.	Antécédents au comportement de plainte	118
2.	Réponses pour la protection de la vie privée	121
2.1.	Taxonomie des réponses pour la protection des données personnelles	121
2.2.	Retour critique sur les comportements de réponse face à une violation de la vie privée	123
2.2.1.	Proposition d'une nouvelle classification des réponses à une violation de la vie privée	123
2.2.2.	Antécédents au comportement de réponse	124
Section 3.	Culture et valeurs culturelles	126
1.	Définition du concept de culture	127
1.1.	Développement historique du concept de culture	127

1.1.1.	<i>Culture et anthropologie à partir du XVIIIème siècle</i>	127
1.1.2.	<i>Culture et fait social à partir de Durkheim</i>	129
1.2.	Distinction entre culture et contexte	130
1.3.	Distinction entre niveaux explicites et implicites de la culture	132
2.	Définition et compréhension des valeurs culturelles	135
2.1.	Définition des valeurs culturelles	135
2.2.	Valeurs et processus de socialisation	137
3.	Théories et structures de modèles de valeurs culturelles	140
3.1.	Contributions majeures à la théorie des dimensions culturelles	140
3.2.	Théorie des dimensions de la culture nationale d'Hofstede	141
3.3.	Focus sur la dimension d'individualisme	142
3.4.	Théorie des valeurs de Schwartz	145
3.4.1.	<i>Héritage des valeurs terminales et instrumentales de Rokeach</i>	145
3.4.2.	<i>Valeurs de Schwartz : universelles et reliées entre elles</i>	145
3.4.3.	<i>Valeurs culturelles de Schwartz et comparaison avec les dimensions d'Hofstede</i>	150
3.5.	Diversité et pertinence de nouvelles approches de valeurs	151
3.6.	Retours critiques sur les différents modèles de valeurs culturelles	152
3.6.1.	<i>Critiques possibles du modèle d'Hofstede</i>	152
3.6.2.	<i>Réflexions sur l'ensemble des modèles existants</i>	153
3.6.3.	<i>Nécessité d'une approche macro, méso et micro</i>	154
Chapitre 3.	Cadre général de la thèse	158
Section 1.	Questions de recherche et cadre théorique général	159
1.	Synthèse du contexte et des fondements théoriques	159
2.	Trois niveaux d'observation : macro, méso et micro	161
2.1.	Théorie des échelles d'observation (Desjeux, 2006)	161
2.2.	Niveau macro	162
2.3.	Niveau micro	162
2.4.	Niveau méso	163
2.5.	Trois niveaux au regard de notre question de recherche	164
3.	Modèle conceptuel	166
Section 2.	Positionnement épistémologique et méthodologies de recherche	167
1.	Différence entre positivisme et interprétativisme	167
2.	Approche post-positiviste	168
2.1.	Définition du post-positivisme	168
2.2.	Post-positivisme et cohérence avec mon approche personnelle	169
2.3.	Pertinence du post-positivisme pour notre sujet	170
3.	Méthodologies de recherche	171
Section 3.	Structure de la thèse et apports de chaque essai	173
1.	Description et objectifs de chaque essai	173
2.	Apports de chaque essai à la thèse	175
3.	Contributions des auteurs et stade d'avancement dans la publication des essais	177
Chapitre 4.	Essai 1 - Influence de la culture nationale	182
Section 1.	Introduction et fondements de la recherche	183
1.	Introduction	183
2.	Fondements théoriques	186
2.1.	Souci de contrôle de ses données personnelles et « contrat social »	186
2.2.	Comportement de plainte individuelle	188
2.3.	Modèle de la culture nationale d'Hofstede	189
3.	Étude exploratoire de la culture nationale en Europe	191
Section 2.	Modèle conceptuel et hypothèses de recherche	193

1. Individualisme et plainte pour protection des données personnelles	193
2. Masculinité et plainte pour protection des données personnelles	194
3. Orientation à long terme et plainte pour protection des données personnelles	195
Section 3. Recherche empirique et résultats	197
1. Méthodologie	197
2. Première étape de l'analyse.....	199
3. Deuxième étape de l'analyse	200
Section 4. Discussion et implications.....	202
1. Contributions théoriques.....	202
1.1. Au-delà de la discussion « Individualisme culturel – protection de la vie privée »	202
1.2. Identification d'un comportement de plainte spécifique.....	203
2. Implications pratiques	203
2.1. Vers une adaptation locale des moyens d'adoption du RGPD	203
2.2. Vers la construction d'une typologie de pays européens.....	205
3. Limites et voies de recherches.....	206
Chapitre 5. Essai 2 - Influence des normes socio-culturelles	212
Section 1. Introduction.....	213
Section 2. Fondements théoriques de la recherche.....	218
1. Valeurs et motivations socio-culturelles.....	218
2. Réponses engagées pour la protection des données personnelles	219
2.1. Engagement face à une violation de données personnelles	219
2.2. Réponses face à une violation de données personnelles.....	220
3. Théorie de la pratique	221
3.1. Principes généraux de la théorie de la pratique.....	221
3.2. Théorie de la pratique selon Bourdieu	223
3.3. Théorie de la pratique et la notion de structure de Giddens	224
3.4. Mise en application de la théorie de la pratique	225
4. Facteurs influençant les réponses pour la protection de la vie privée	226
4.1. Antécédents aux réponses de protection de la vie privée	226
4.2. Effets psychologiques des violations de données personnelles	228
4.3. Voies de recherche	229
Section 3. Méthodologie et recherche empirique.....	231
1. Approche qualitative	232
2. Procédure de recrutement.....	232
2.1. Procédure de recrutement.....	232
2.2. Questionnaire préalable à l'entretien.....	233
3. Procédure d'entretiens	236
4. Méthode d'analyse	238
4.1. Comparaison des méthodes d'analyse envisagées.....	238
4.1.1. Méthode 1 : analyse thématique de contenu classique	238
4.1.2. Méthode 2 : chaînes Moyens-Fins	239
4.1.3. Méthode 3 : analyse textuelle automatique.....	240
4.1.4. Comparatif des méthodes	241
4.2. Procédure d'analyse choisie	242
4.2.1. Analyse de contenu et établissement des codes.....	243
4.2.2. Méthode de chaînage cognitif.....	244
4.2.3. Analyse des pratiques sociales de protection de la vie privée	245
Section 4. Résultats descriptifs de la recherche	246
1. Actions de protection de la vie privée	246
1.1. Actions techniques	247

1.1.1.	<i>Protection technique</i>	248
1.1.2.	<i>Brouillage digital</i>	248
1.1.3.	<i>Hygiène digitale</i>	248
1.1.4.	<i>Avantages et inconvénients des réponses techniques</i>	250
1.2.	Actions sociales	251
1.2.1.	<i>Formation support</i>	251
1.2.2.	<i>Sensibilisation des proches</i>	252
1.2.3.	<i>Name and shame</i>	252
1.2.4.	<i>Militantisme</i>	252
1.2.5.	<i>Caractéristiques des réponses sociales</i>	254
1.3.	Actions institutionnelles	255
1.3.1.	<i>Signalement à l'entreprise</i>	255
1.3.2.	<i>Plainte à la CNIL</i>	256
1.3.3.	<i>Recours en justice</i>	258
1.4.	Réponses face à une violation de données personnelles	259
2.	Conséquences et valeurs culturelles identifiées	260
Section 5.	Résultats analytiques de la recherche	263
1.	Motivations socio-culturelles dominantes	263
1.1.	<i>Équité sociale : première motivation culturelle</i>	263
1.2.	<i>Liberté : deuxième motivation culturelle</i>	267
1.3.	<i>Sécurité : troisième motivation culturelle</i>	269
2.	Pratiques sociales de protection de la vie privée	271
2.1.	<i>Dynamiques structurelles des pratiques de protection de la vie privée</i>	271
2.2.	<i>Formes de compétences individuelles pour la protection de la vie privée</i>	274
2.2.1.	<i>Distance psychologique avec les risques liés à la violation de la vie privée</i>	275
2.2.2.	<i>Alphabétisation en matière de vie privée</i>	276
2.2.3.	<i>Efficacité personnelle en matière de vie privée</i>	277
2.2.4.	<i>Fatigue liée à la protection de vie privée</i>	278
2.3.	<i>Formes de compétences collectives pour la protection de la vie privée</i>	280
Section 6.	Discussion et implications	282
1.	Contributions théoriques	283
1.1.	<i>Approche de la protection de la vie privée par la théorie de la pratique</i>	283
1.2.	<i>Remise en question d'une préférence à l'individualisme dans le cadre de la protection de la vie privée</i>	285
2.	Implications pratiques	286
3.	Limites et voies de recherches	286
Chapitre 6. Essai 3 - Influence des orientations culturelles individuelles..	290	
Section 1.	Introduction et fondements de la recherche	291
1.	Introduction	291
2.	Fondements théoriques	295
2.1.	<i>Violations de données personnelles et réponses de protection du consommateur</i>	295
2.1.1.	<i>Définition des violations de données personnelles</i>	295
2.1.2.	<i>Réponses aux violations de données personnelles</i>	295
2.1.3.	<i>Mécanismes psychologiques à l'œuvre dans la réponse face à une violation de données personnelles</i>	296
2.2.	<i>Préoccupation pour la protection des données personnelles</i>	297
2.3.	<i>Distance psychologique et préoccupations pour la protection des données personnelles</i>	298
2.3.1.	<i>Théorie de la distance psychologique</i>	298
2.3.2.	<i>Distance psychologique et consommation</i>	299
2.3.3.	<i>Distance psychologique et préoccupation pour la protection des données personnelles</i>	300
2.4.	<i>Culture et orientations culturelles individuelles</i>	303
2.4.1.	<i>Culture et valeurs culturelles</i>	303
2.4.2.	<i>Modèles de mesures des valeurs culturelles</i>	303
2.4.3.	<i>Définitions des grandes orientations culturelles</i>	305

Section 2. Modèle conceptuel et développement des hypothèses.....	308
1. Distance psychologique et préoccupation pour la protection de la vie privée	308
1.1. Application de la distance psychologique aux violations de données personnelles.....	308
1.2. Préoccupation pour la protection des données personnelles et distance psychologique avec la violation de données personnelles.....	309
2. Influence des orientations culturelles individuelles	310
2.1. Influence de l'indépendance.....	310
2.2. Influence de l'inégalité sociale	313
2.3. Influence de l'aversion au risque.....	314
2.4. Influence de l'égalité des genres	315
2.5. Influence de l'orientation vers la tradition	317
3. Réponses face à une violation de données personnelles.....	318
Section 3. Recherche empirique et résultats	320
1. Méthodologie	320
1.1. Choix des échelles.....	320
1.2. Construction de scénarios	322
1.3. Variables de contrôle	324
1.4. Échantillon.....	325
1.5. Ajustement des échelles	326
2. Résultats.....	327
2.1. Fréquences de violations de données.....	327
2.2. Méthodes d'équations structurelles, ajustement global du modèle et indices de validité.....	327
2.3. Invariance des mesures.....	328
2.4. Tests des hypothèses	329
2.5. Variables de contrôle	330
Section 4. Discussion et implications.....	333
1. Contributions théoriques.....	334
2. Implications pratiques	335
2.1. Vers des actions adaptées aux groupes sociaux et à leurs préférences en termes de valeurs culturelles	335
2.2. Vers un exercice du droit plus collectif.....	335
2.3. Vers des actions de communication plus adaptées.....	336
3. Limites et voies de recherche	337
Chapitre 7. Discussion et conclusion	342
Section 1. Contributions théoriques.....	344
1. Effets culturels sur les réponses aux violations de données personnelles	346
1.1. Préférence culturelle pour des valeurs d'équité sociale et de genre.....	347
1.2. Compréhension d'une préférence culturelle pour l'individualité autour de deux axes : liberté et sécurité	348
2. Réponses aux violations de données personnelles	349
2.1. Proposition d'une typologie de réponses de protection de la vie privée	349
2.2. Compréhension d'un comportement de plainte spécifique : la plainte au régulateur	350
3. Distance psychologique avec la protection de la vie privée.....	351
4. Théorie de la pratique et pratiques de protection de la vie privée	353
4.1. Nouveau cadre théorique appliqué à la protection de la vie privée	353
4.2. Compréhension des phénomènes de changement, d'engagement et de résistance	354
4.2.1. Compréhension des phénomènes reliant macro et micro	354
4.2.2. Théorie de la pratique, effets d'engagement et de résistance	355
5. Nouvelle compréhension du souci de protection de la vie privée	356
5.1. Fondements individuels du souci de contrôle des données personnelles	356
5.2. Limites d'une sur-individualisation du contrôle des données personnelles	357
5.3. Pertes de contrôle et de transparence : réponses du consommateur en situation de vulnérabilité informatique.....	359
5.4. Proposition de nouvelle définition pour la protection de la vie privée.....	361

Section 2. Implications pratiques	362
1. Développement de pratiques de protection de la vie privée.....	363
1.1. Structure de la pratique sociale de la protection de la vie privée.....	363
1.2. Applications concrètes pour le développement de pratiques de protection de la vie privée	364
1.2.1. Identification d'actions concernant les valeurs, matériaux et formes de compétences	364
1.2.2. Actions qui agissent conjointement.....	365
1.2.3. Dynamique basée sur le méso	366
1.3. Acteurs de la pratique sociale de la protection de la vie privée.....	368
2. Discours médiatique et publicitaire.....	372
2.1. Discours publicitaires mobilisant les préférences motivationnelles	372
2.2. Réduction de la distance psychologique avec les violations de données personnelles	373
2.3. Utilisation de dynamiques collectives.....	376
3. Évolutions réglementaires	377
3.1. Adaptation locale des réglementations internationales	377
3.2. Nécessité de possibilités de plaintes collectives.....	378
3.3. Efficacité des moyens de recours au droit en vue d'une indemnisation des victimes	379
Section 3. Limites et voies de recherche	380
1. Protection des données personnelles et de la vie privée.....	380
1.1. Compréhension théorique de la pratique	380
1.2. Compréhension théorique de la distance psychologique.....	382
1.3. Approfondissement du lien entre vie privée et cybersécurité	382
2. Réponses apportées aux violations de données personnelles	383
2.1. Définitions des violations de données personnelles en marketing	383
2.2. Lien entre préjudice, réponses et dédommagement	384
2.3. Violations de données dans un contexte de publicité digitale	385
3. Culture et souci de protection de la vie privée	386
3.1. Compréhension des effets culturels sur la protection de la vie privée dans des pays émergents	386
3.2. Application aux problématiques de transferts internationaux de données.....	387
Conclusion générale	389
Liste des tableaux.....	393
Liste des figures.....	395
Tables des annexes	397
Tables des matières	398
Références bibliographiques	405
Annexes	426

Références bibliographiques

- Aaron Gabisch, J., & R. Milne, G. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing*, 31(1), 13-26. <https://doi.org/10.1108/JCM-10-2013-0737>
- Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce* (pp.21-29). <https://dl.acm.org/doi/pdf/10.1145/988772.988777>
- Acquisti, A. (2009). Nudging Privacy : The Behavioral Economics of Personal Information. *IEEE Security & Privacy Magazine*, 7(6), 82-85. <https://doi.org/10.1109/MSP.2009.163>
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes : The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, 30(4), 736-758. <https://doi.org/10.1002/jcpy.1191>
- Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches ? An event study. *ICIS 2006 proceedings*, 94.
- Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences*, 106(27), 10975-10980. <https://doi.org/10.1073/pnas.0904891106>
- Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, 31(2), 96-110. <https://doi.org/10.1080/08911762.2017.1412552>
- Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of retailing*, 91(1), 34-49.
- Ahmadi, I., Habel, J., Jia, M., Lee, N., & Wei, S. (2022). Consumer stockpiling across cultures during the COVID-19 pandemic. *Journal of International Marketing*, 30(2), 28-37. <https://doi.org/10.1177/1069031X211037590>
- Ailon, G. (2008). Mirror, Mirror on the Wall : Culture's Consequences in A Value Test of its Own Design. *Academy of Management Review*, 33(4), 885-904. <https://doi.org/10.5465/amr.2008.34421995>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179-211.
- Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological bulletin*, 82(2), 261-277.
- Akaka, M. A., Vargo, S. L., & Lusch, R. F. (2013). The Complexity of Context : A Service Ecosystems Approach for International Marketing. *Journal of International Marketing*, 21(4), 1-20. <https://doi.org/10.1509/jim.13.0032>
- Alkis, A., & Kose, T. (2022). Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. *Computers in Human Behavior*, 137, 107412.
- Allard-Poesi, F. (2003). Coder les données. In Y. Giordano, *Conduire un projet de recherche, une perspective qualitative* (pp. 245-290). Ed. EMS.
- Allard-Poesi, F., & Perret, V. (2014). Chapitre 1. Fondements épistémologiques de la recherche. In Thiéart, R. A., *Méthodes de recherche en management* (pp.14-16). Ed. Dunod.
- Altman, I. (1975). The Environment and Social Behavior : Privacy, Personal Space, Territory, and Crowding.
- Altman, I. (1977). Privacy Regulation : Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33(3), 66-84. <https://doi.org/10.1111/j.1540-4560.1977.tb01883>
- Andreasen, A. R., & Best, A. (1977). *Consumers Complain—Does Business Respond?* Harvard Business Review.
- Ariès, P., & Duby, G. (1985). *Histoire de la vie privée*, 5 tomes. Paris, Éditions du Seuil.
- Arpagian, N. (2022). *La cybersécurité*. Que sais-je.

- Aubert-Hassouni, C., & Cloarec, J. (2022). Privacy regulation in the age of Digital Marketing. In Hanlon, A., & Tuten, T. L., *The SAGE Handbook of Digital Marketing* (pp. 544-556). SAGE Publications Ltd.
- Aurifeille, J. M. (1993). La segmentation par les chaînes moyens-fins : Méthodologie et validité prédictive. *Congrès International de l'Association Française du Marketing* (pp.363-394).
- Austin, W., & Walster, E. (1974). Reactions to confirmations and disconfirmations of expectancies of equity and inequity. *Journal of Personality and Social Psychology*, 30(2), 208-216.
- Bach, S. B., & Kim, S. (2012). Online Consumer Complaint Behaviors : The Dynamics of Service Failures, Consumers' Word of Mouth, and Organization-Consumer Relationships. *International Journal of Strategic Communication*, 6(1), 59-76. <https://doi.org/10.1080/1553118X.2011.634871>
- Baker-Eveleth, L., Stone, R., & Eveleth, D. (2022). Understanding social media users' privacy-protection behaviors. *Information & Computer Security*, 30(3), 324-345.
- Balakrishnan, J., Abed, S. S., & Jones, P. (2022). The role of meta-UTAUT factors, perceived anthropomorphism, perceived intelligence, and social self-efficacy in chatbot-based services? *Technological Forecasting and Social Change*, 180, 121692. <https://doi.org/10.1016/j.techfore.2022.121692>
- Balbo, L., & Jeannot, F. (2015). L'adéquation du cadrage du message et de la distance temporelle : Un moyen efficace de promouvoir un produit innovant. *Recherche et Applications en Marketing (French Edition)*, 30(1), 28-51. <https://doi.org/10.1177/0767370114552937>
- Balech, S., & Benavent, C. (2019). *NLP text mining V4.0—Une introduction—Cours programme doctoral*. <https://doi.org/10.13140/RG.2.2.34248.06405>
- Ballantyne, D., Christopher, M., & Payne, A. (1995). Improving the quality of services marketing : Service (Re) design is the critical link. *Journal of Marketing Management*, 11(1-3), 7-24. <https://doi.org/10.1080/0267257X.1995.9964326>
- Bandara, R. J., Fernando, M., & Akter, S. (2018). Is the Privacy Paradox a Matter of Psychological Distance? An Exploratory Study of the Privacy Paradox from a Construal Level Theory Perspective. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018 (pp. 3678-3687).
- Bandara, R. J., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox : A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, 52, 101947. <https://doi.org/10.1016/j.jretconser.2019.101947>
- Bandara, R. J., Fernando, M., & Akter, S. (2021). Construing online consumers' information privacy decisions : The impact of psychological distance. *Information & Management*, 58(7), 103497. <https://doi.org/10.1016/j.im.2021.103497>
- Bandura, A. (1977). Self-efficacy : Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215.
- Bansal, G., & Nah, F. F. H. (2022). Internet privacy concerns revisited : oversight from surveillance and right to be forgotten as new dimensions. *Information & Management*, 59(3), 103618. <https://doi.org/10.1016/j.im.2022.103618>
- Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair : The information privacy perspective. *Decision Support Systems*, 71, 62-77. <https://doi.org/10.1016/j.dss.2015.01.009>
- Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 24(6), 624-644. <https://doi.org/10.1057/ejis.2014.41>
- Barnes, J. G., & Kelloway, K. R. (1980). Consumerists : Complaining Behavior and Attitudes Toward Social and Consumer Issues. *ACR North American Advances*, 7, 329-334, <https://www.acrwebsite.org/volumes/9692/volumes/v07/NA-07/full>
- Bartsch, M., & Dienlin, T. (2016). Control your Facebook : An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147-154. <https://doi.org/10.1016/j.chb.2015.11.022>
- Baudet, S. (1990). Représentations cognitives d'état, d'événement et d'action. *Langages*, 25(100), 45-64. <https://doi.org/10.3406/lgge.1990.1566>
- Bearden, W. O., Money, B. R., & Nevins, J. L. (2006). A Measure of Long-Term Orientation : Development and Validation. *Journal of the Academy of Marketing Science*, 34(3), 456-467. <https://doi.org/10.1177/0092070306286706>

- Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy : Current Knowledge and Research Directions. *Foundations and Trends® in Marketing*, 11(1), 1-71. <https://doi.org/10.1561/17000000057>
- Bélanger, F. & Crossler, F.E. (2011). Privacy in the Digital Age : A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017. <https://doi.org/10.2307/41409971>
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce : The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270. [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns : A Global Survey of Consumers. *The Information Society*, 20(5), 313-324. <https://doi.org/10.1080/01972240490507956>
- Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2021). Information Privacy, Cultural Values, and Regulatory Preferences: *Journal of Global Information Management*, 29(3), 131-164. <https://doi.org/10.4018/JGIM.2021050106>
- Bergadaa, M. (1990). The role of time in the Action of consumer. *Journal of Consumer Research*, 17(3), 289-302. 2.
- Billings, R. S., Milburn, T. W., & Schaalman, M. L. (1980). A Model of Crisis Perception : A Theoretical and Empirical Analysis. *Administrative Science Quarterly*, 25(2), 300-316. <https://doi.org/10.2307/2392456>
- Bilsky, W., & Schwartz, S. H. (1994). Values and personality. *European Journal of Personality*, 8(3), 163-181. <https://doi.org/10.1002/per.2410080303>
- Binninger, A.-S., & Robert, I. (2008). Consommation et développement durable : Vers une segmentation des sensibilités et des comportements. *La Revue des Sciences de Gestion*, 229(1), 51-59. <https://doi.org/10.3917/rsg.229.0051>
- Boroditsky, L. (2000). Metaphoric structuring : Understanding time through spatial metaphors. *Cognition*, 75(1), 1-28. [https://doi.org/10.1016/S0010-0277\(99\)00073-6](https://doi.org/10.1016/S0010-0277(99)00073-6)
- Boroditsky, L., & Ramscar, M. (2002). The Roles of Body and Mind in Abstract Thought. *Psychological Science*, 13(2), 185-189.
- Boudon, R. (1984). L'individualisme méthodologique en sociologie. *Commentaire*, 26(2), 268-277. <https://doi.org/10.3917/comm.026.0268>
- Boudon, R. (2002). Utilité ou rationalité? Rationalité restreinte ou générale? *Revue d'économie politique*, 755-772.
- Boudon, R., & Bourricaud, F. (1982). *Dictionnaire critique de la sociologie*. Puf.
- Bourdieu, P. (1972). *Esquisse d'une théorie de la pratique*. Librairie Droz.
- Bourdieu, P. (1979). *La Distinction, critique sociale du jugement*. Les Éditions de Minuit.
- Bourdieu, P. (2016). *Méditations pascaliennes*. Média Diffusion.
- Bourqia, R. (2006). *Les valeurs, changements et perspectives*.
- Bourqia, R. (2010). Valeurs et changement social au Maroc. *Quaderns de la Mediterrània*, 13(2010), 105-115.
- Brady, M., Knight, G., Croninjr, J., Tomas, G., Hult, M., & Keillor, B. (2005). Removing the contextual lens : A multinational, multi-setting comparison of service evaluation models. *Journal of Retailing*, 81(3), 215-230. <https://doi.org/10.1016/j.jretai.2005.07.005>
- Bréchon, P. (2019). L'évolution des valeurs : À propos du livre de Ronald Inglehart. Les Transformations culturelles. Comment les valeurs des individus bouleversent le monde ? *Futuribles*, 428(1), 17-31. <https://doi.org/10.3917/futur.428.0017>
- Brewer, P., & Venaik, S. (2012). On the misuse of national culture dimensions. *International Marketing Review*, 29(6), 673-683. <https://doi.org/10.1108/02651331211277991>
- Brough, A. R., & Martin, K. D. (2021). Consumer Privacy During (and After) the COVID-19 Pandemic. *Journal of Public Policy & Marketing*, 40(1), 108-110. <https://doi.org/10.1177/0743915620929999>
- Brügger, A., Morton, T. A., & Dessai, S. (2016). "Proximising" climate change reconsidered : A construal level theory perspective. *Journal of Environmental Psychology*, 46, 125-142. <https://doi.org/10.1016/j.jenvp.2016.04.004>

- Buehler, R., Griffin, D., & Ross, M. (1994). Exploring the "planning fallacy": Why people underestimate their task completion times. *Journal of personality and social psychology*, 67(3), 366-381.
- Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of social and personal relationships*, 6(2), 131-158.
- Burnett, J. J. (1998). A strategic approach to managing crises. *Public Relations Review*, 24(4), 475-488. [https://doi.org/10.1016/S0363-8111\(99\)80112-X](https://doi.org/10.1016/S0363-8111(99)80112-X)
- Butori, R., & Parguel, B. (2010). When students give biased responses to researchers: An exploration of traditional paper vs. computerized self-administration, *European Marketing Academy Conference*, Copenhagen, Denmark.
- Cao, J., & Everard, A. (2008). User Attitude Towards Instant Messaging : The Effect of Espoused National Cultural Values on Awareness and Privacy. *Journal of Global Information Technology Management*, 11(2), 30-57. <https://doi.org/10.1080/1097198X.2008.10856466>
- Carbou, G. (2017). Quelques questions à l'attention des utilisateurs de statistique textuelle pour l'analyse des discours. *Texte! Textes et cultures*, 22(4).
- Cardon, D. (2019). *Culture numérique*. SciencesPo les presses.
- Catinaud, R. (2015). Qu'est-ce qu'une pratique? : Théories et théorisation des pratiques [Doctoral dissertation, University of Geneva].
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value : Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), 70-104. <https://doi.org/10.1080/10864415.2004.11044320>
- Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change*, 96, 277-287. <https://doi.org/10.1016/j.techfore.2015.01.021>
- Chamaret, C., Steyer, V., & Mayer, J. C. (2020). "Hands off my meter!" when municipalities resist smart meters : Linking arguments and degrees of resistance. *Energy Policy*, 144, 111556. <https://doi.org/10.1016/j.enpol.2020.111556>
- Chan, E. Y., & Palmeira, M. (2021). Political ideology moderates consumer response to brand crisis apologies for data breaches. *Computers in Human Behavior*, 121, 106801. <https://doi.org/10.1016/j.chb.2021.106801>
- Chandrasekharan, E., Samory, M., Jhaver, S., Charvat, H., Bruckman, A., Lampe, C., Eisenstein, J., & Gilbert, E. (2018). The Internet's Hidden Rules : An Empirical Study of Reddit Norm Violations at Micro, Meso, and Macro Scales. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1-25. <https://doi.org/10.1145/3274301>
- Chapa, O., Hernandez, M. D., Wang, Y. J., & Skalski, C. (2014). Do Individualists Complain More than Collectivists? A Four-Country Analysis on Consumer Complaint Behavior. *Journal of International Consumer Marketing*, 26(5), 373-390. <https://doi.org/10.1080/08961530.2014.933089>
- Charreire-Petit, S., & Durieux, F. (2007). Explorer et tester : Les deux voies de la recherche. In Thiétart, R. A., *Méthodes de recherche en management* (pp.58-83). Ed. Dunod.
- Chataigné, C. (2014). *Psychologie des valeurs*. De Boeck Supérieur.
- Chaudhury, S. R., & Albinsson, P. A. (2015). Citizen-Consumer Oriented Practices in Naturalistic Foodways : The Case of the Slow Food Movement. *Journal of Macromarketing*, 35(1), 36-52. <https://doi.org/10.1177/0276146714534264>
- Chazel, F. (1991). Chapitre 9. Individualisme, mobilisation et action collective. In Birnbaum, P., & Leca, J., *Sur l'individualisme, théories et méthodes* (pp. 244-268). Presses de Sciences Po. <https://doi.org/10.3917/scpo.birnb.1991.01.0244>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy : An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), 181-202. <https://doi.org/10.1007/s10799-005-5879-y>
- Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, 18(1), 13-19.

- Chen, J. Q., Zhang, R., & Lee, J. (2013). A Cross-Culture Empirical Study of M-commerce Privacy Concerns. *Journal of Internet Commerce*, 12(4), 348-364.
<https://doi.org/10.1080/15332861.2013.865388>
- Chin, W. W., Mills, A. M., Steel, D. J., & Schwarz, A. (2016). Multi-group invariance testing : An illustrative comparison of PLS permutation and covariance-based SEM invariance analysis. In *The Multiple Facets of Partial Least Squares and Related Methods: PLS, Paris, France, 2014* 8 (pp.267-284). Springer International Publishing.
- Chiu, C-Y., & Hong, Y-Y. (2007), Chap. 34, Cultural Processes, basic principles, In Kruglanski, A. W., & Higgins, E. T., *Social psychology : Handbook of basic principles (2nd ed)*. Guilford Press.
- Cho, H., Li, P., & Goh, Z. H. (2020). Privacy Risks, Emotions, and Social Media : A Coping Model of Online Privacy. *ACM Transactions on Computer-Human Interaction*, 27(6), 1-28.
<https://doi.org/10.1145/3412367>
- Cho, H., Rivera-Sánchez, M., & Sun Sun Lim. (2009). A multinational study on online privacy : Global concerns and local responses. *New Media & Society*, 11(3), 395-416.
<https://doi.org/10.1177/1461444808101618>
- Chognot, C. (2020). 5. Le niveau méso comme levier de la dimension de mouvement. In Chognot, C., *Le sens de l'action dans les associations* (pp. 115-163). Collection sociologie économique. Ed. Érès.
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51. <https://doi.org/10.1016/j.chb.2017.12.001>
- Cialdini, R. B. (1993). *Influence: Science and Practice*, New York: HarperCollins.
- Citron, D. K., & Solove, D. J. (2022). Privacy harms. *BUL Rev.*, 102, 793.
- Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67.
- Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, 161, 120299. <https://doi.org/10.1016/j.techfore.2020.120299>
- Cloarec, J. (2022). Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. *Journal of Business Research*, 152, 144-153.
<https://doi.org/10.1016/j.jbusres.2022.07.045>
- Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2022). The personalization–privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, 39(3), 647-661. <https://doi.org/10.1002/mar.21587>
- Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content : A corporate reputation analysis. *European Management Journal*, 37(4), 492-504. <https://doi.org/10.1016/j.emj.2019.01.007>
- Cooper, M. M. (1997). Distinguishing Critical and Post-Positivist Research. *College Composition and Communication*, 48(4), 556-561. <https://doi.org/10.2307/358458>
- Cornwell, T. B., Bligh, A. D., & Babakus, E. (1991). Complaint Behavior of Mexican-American Consumers to a Third-Party Agency. *Journal of Consumer Affairs*, 25(1), 1-18.
<https://doi.org/10.1111/j.1745-6606.1991.tb00278.x>
- Crié, D. (2003). Consumers' complaint behaviour. Taxonomy, typology and determinants : Towards a unified ontology. *Journal of Database Marketing & Customer Strategy Management*, 11(1), 60-79. <https://doi.org/10.1057/palgrave.dbm.3240206>
- Cuche, D. (2020). *La notion de culture dans les sciences sociales*. La Découverte.
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy : Balancing economic and justice considerations. *Journal of social issues*, 59(2), 323-342.
- Culnan, M. J., & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy : Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly*, 33(4), 673-687.
<https://doi.org/10.2307/20650322>
- Darke, P. R., Brady, M. K., Benedictus, R. L., & Wilson, A. E. (2016). Feeling Close From Afar : The Role of Psychological Distance in Offsetting Distrust in Unfamiliar Online Retailers. *Journal of Retailing*, 92(3), 287-299. <https://doi.org/10.1016/j.jretai.2016.02.001>
- Davidson, D. (1980). *Actions et événements*, traduction P. Engel, Paris, PUF.

- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3), 319-340.
- Day, R. L. (1977). Extending the concept of consumer satisfaction. *ACR North American Advances*, 4, 149-154. <https://www.acrwebsite.org/volumes/9346/volumes/vol4/NA-04>
- Day, R. L., Grabicke, K., Schaetzle, T., & Staubach, F. (1981). The hidden agenda of consumer complaining. *Journal of Retailing*, 57(3), 86-106.
- Day, R. L., & Landon, E. L. (1977). Toward a theory of consumer complaining behavior. *Consumer and industrial buying behavior*, 95(1), 425-437.
- Del Bucchia, C., Miltgen, C. L., Russell, C. A., & Burlat, C. (2021). Empowerment as latent vulnerability in techno-mediated consumption journeys. *Journal of Business Research*, 124, 629-651. <https://doi.org/10.1016/j.jbusres.2020.03.014>
- De Guttry, C., Doring, M., & Ratter, B. (2017). How Distant is Climate Change? Construal Level Theory Analysis of German and Taiwanese Students Statements. *International Journal of Asian Social Science*, 7(5), 434-447. <https://doi.org/10.18488/journal.1.2017.75.434.447>
- De Mooij, M. (2017). Comparing dimensions of national culture for secondary analysis of consumer behavior data of different countries. *International Marketing Review*, 34(3), 444-456. <https://doi.org/10.1108/IMR-02-2016-0047>
- Denis, M., & Le Ny, J.-F. (1993). *Modèles et concepts pour la science cognitive : Hommage à Jean-François Le Ny*. Presses Univ. de Grenoble.
- Denzin, N. K., & Lincoln, Y. S. (2008). Introduction : The discipline and practice of qualitative research. In *Strategies of qualitative inquiry*, 3rd ed (pp. 1-43). SAGE Publications, Inc.
- Desjeux, D. (2006). La question des échelles d'observation en sciences humaines appliquées au domaine de la santé. *Recherche en soins infirmiers*, 85(2), 14-21.
- Diderot, D., & Alembert, J. L. R. d'. (1777). Encyclopédie Pellet.
- Didi Alaoui, M., & Cova, V. (2021). La distance psychologique comme outil actionnable par les managers. *Recherche et Applications en Marketing (French Edition)*, 1(25). <https://doi.org/10.1177/0767370121992803>
- Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way* (pp. 59). Springer. <https://doi.org/10.1007/978-3-030-30371-6>
- Dimanche, F., & Havitz, M. E. (1995). Consumer Behavior and Tourism. *Journal of Travel & Tourism Marketing*, 3(3), 37-57. https://doi.org/10.1300/J073v03n03_03
- Dinev, T. & Hart, P. (2006). Privacy Concerns and Levels of Information Exchange : An Empirical Investigation of Intended e-Services Use. *E-Service Journal*, 4(3), 25-59. <https://doi.org/10.2979/esj.2006.4.3.25>
- Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, 23(2), 97-102. <https://doi.org/10.1057/ejis.2014.1>
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402. <https://doi.org/10.1057/palgrave.ejis.3000590>
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413-422. <https://doi.org/10.1080/01449290410001715723>
- Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics : Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4), 639-655. <https://doi.org/10.1287/isre.2015.0600>
- D'Iribarne, P., Henry, A., Segal, J.-P., Chevrier, S., & Globokar, T. (1998). *Cultures et mondialisation. Gérer par-delà les frontières*. Éditions du Seuil.
- Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: integrative social contracts theory. *Academy of Management Review*, 10(2), 252-284.
- Donthu, N., & Yoo, B. (1998). Cultural influences on service quality expectations. *Journal of service research*, 1(2), 178-186.
- Dopfer, K., Foster, J., & Potts, J. (2004). Micro-meso-macro. *Journal of Evolutionary Economics*, 14(3), 263-279. <https://doi.org/10.1007/s00191-004-0193-0>

- Dozier, J. B., & Miceli, M. P. (1985). Potential Predictors of Whistle-Blowing : A Prosocial Behavior Perspective. *The Academy of Management Review*, 10, 823-836.
<https://doi.org/10.2307/258050>
- Dubuisson-Quellier, S., & Plessz, M. (2013). La théorie des pratiques. *Sociologie*, 4(4).
<https://journals.openedition.org/sociologie/2030>
- Dumez, H. (2021). *Méthodologie de la recherche qualitative : Toutes les questions clés de la démarche*. Vuibert.
- Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social contracts and marketing ethics. *Journal of marketing*, 63(3), 14-32.
- Durkheim, É. (1894). Les règles de la méthode sociologique. *Revue Philosophique de la France et de l'Étranger*, 37, 465-498.
- Durkheim, É. (1909). Elemente der Voelkerpsychologie. Grundlinien einer psychologischen Entwicklungsgeschichte der Menschheit. *L'Année sociologique (1896/1897-1924/1925)*, 12ème année, 50-61.
- Eberl, M. (2010). An application of PLS in multi-group analysis : The need for differentiated corporate-level marketing in the mobile communications industry. In Vinzi, V. E., Chin, W. W., Henseler, J., & Wang, H., *Handbook of partial least squares : Concepts, methods and applications* (pp. 487-514). Springer.
- Eggers, F., Beke, F. T., Verhoef, P. C., & Wieringa, J. E. (2022). The market for privacy : Understanding how consumers trade off privacy practices. *Journal of Interactive Marketing*.
- Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults : Westin's privacy attitude typology revisited. *American Behavioral Scientist*, 62(10), 1372-1391.
- Etzioni, A. (2004). *How Patriotic is the Patriot Act? : Freedom Versus Security in the Age of Terrorism*. Routledge. <https://doi.org/10.4324/9780203997130>
- Eyal, T., Sagristano, M. D., Trope, Y., Liberman, N., & Chaiken, S. (2009). When values matter : Expressing values in behavioral intentions for the near vs. distant future. *Journal of Experimental Social Psychology*, 45(1), 35-43. <https://doi.org/10.1016/j.jesp.2008.07.023>
- Farhangmehr, M., & Silva, M. (1995). Strategic importance of consumer's complaints : An empirical study. *Marketing today and for the 21th century*, 1595, 1604.
- Fiedler, K., Jung, J., Wänke, M., & Alexopoulos, T. (2012). On the relations between distinct aspects of psychological distance : An ecological basis of construal-level theory. *Journal of Experimental Social Psychology*, 48(5), 1014-1021. <https://doi.org/10.1016/j.jesp.2012.03.013>
- Fischer, R., & Schwartz, S. (2011). Whence Differences in Value Priorities? : Individual, Cultural, or Artifactual Sources. *Journal of Cross-Cultural Psychology*, 42(7), 1127-1144.
<https://doi.org/10.1177/0022022110381429>
- Fischer, R., Vauclair, C.-M., Fontaine, J. R., & Schwartz, S. H. (2010). Are individual-level and country-level value structures different? Testing Hofstede's legacy with the Schwartz Value Survey. *Journal of cross-cultural psychology*, 41(2), 135-151.
- Fishbein, M., & Ajzen, I. (1980). Predicting and understanding consumer behavior : Attitude-behavior correspondence. *Understanding attitudes and predicting social behavior*, 1(1), 148-172.
- Fishbein, M., & Ajzen, I. (2011). *Predicting and Changing Behavior : The Reasoned Action Approach*. Psychology Press. Taylor & Francis. <https://doi.org/10.4324/9780203838020>
- Fiske, S. T., & Macrae, C. N. (2012). *The SAGE Handbook of Social Cognition*. SAGE.
- Foerderer, J., & Schuetz, S. W. (2022). Data Breach Announcements and Stock Market Reactions : A Matter of Timing? *Management Science*, 68(10), 7298-7322.
<https://doi.org/10.1287/mnsc.2021.4264>
- Fornell, C., & Wernerfelt, B. (1987). Defensive Marketing Strategy by Customer Complaint Management : A Theoretical Analysis. *Journal of Marketing Research*, 24(4), 337-346.
- Fornell, C., & Westbrook, R. A. (1979). An Exploratory Study of Assertiveness, Aggressiveness, and Consumer Complaining Behavior. *ACR North American Advances*, 06, 105-110,
<https://www.acrwebsite.org/volumes/9540/volumes/v06/NA-06/full>
- Foucault, M. (1975). *Surveiller et punir*. Paris.
- Foucault, M. (2001). *Des espaces autres. Dits et écrits II (1976-1988)*. Paris: Gallimard.
- Fukuyama, F. (1995). *Trust : The social virtues and the creation of prosperity*. Free Press. New York.

- Gelbrich, K., Gäthke, J., & Grégoire, Y. (2015). How Much Compensation Should a Firm Offer for a Flawed Service? An Examination of the Nonlinear Effects of Compensation on Satisfaction. *Journal of Service Research*, 18(1), 107-123. <https://doi.org/10.1177/1094670514543149>
- Georges, F. (2009). Représentation de soi et identité numérique : Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0. *Réseaux*, 154(2), 165-193. <https://doi.org/10.3917/res.154.0165>
- Giddens, A. (1976). *New rules of sociological method : A positive critique of interpretative sociologies*. Stanford University Press.
- Giddens, A. (1979). *Central Problems in Social Theory : Action, Structure, and Contradiction in social analysis*. University of California Press.
- Giddens, A. (1984). *The Constitution of Society : Outline of the Theory of Structuration*. Polity press.
- Girerd-Potin, I., Jimenez-Garcès, S., & Louvet, P. (2018). L'influence de la culture nationale sur les politiques socialement responsables des entreprises. *Management international*, 21(4), 146-163. <https://doi.org/10.7202/1053584ar>
- Gorodnichenko, Y., & Roland, G. (2011). Individualism, innovation, and long-run growth. *Proceedings of the National Academy of Sciences*, 108, 21316-21319. <https://doi.org/10.1073/pnas.1101933108>
- Gouveia, V. V., Milfont, T. L., Fischer, R., and Santos, W. S. (2008). Teoria funcionalista dos valores humanos, In M. L. M. Teixeira, *Valores Humanos e Gestão: Novas Perspectivas*, Sao Paulo: Editora Senac, 47-80.
- Greenleaf, G. (2008). Privacy in Australia. In J. Rule & G. Greenleaf, *Global Privacy Protection* (pp. 13251). Edward Elgar Publishing. <https://doi.org/10.4337/9781848445123.00009>
- Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, 2(2), 68-92.
- Grégoire, Y., & Fisher, R. J. (2008). Customer betrayal and retaliation : When your best customers become your worst enemies. *Journal of the Academy of Marketing Science*, 36(2), 247-261. <https://doi.org/10.1007/s11747-007-0054-0>
- Grégoire, Y., Tripp, T. M., & Legoux, R. (2009). When Customer Love Turns into Lasting Hate : The Effects of Relationship Strength and Time on Customer Revenge and Avoidance. *Journal of Marketing*, 73(6), 18-32.
- Grønhaug, K., & Gilly, M. C. (1991). A transaction cost approach to consumer dissatisfaction and complaint actions. *Journal of Economic Psychology*, 12(1), 165-183. [https://doi.org/10.1016/0167-4870\(91\)90048-X](https://doi.org/10.1016/0167-4870(91)90048-X)
- Grønhaug, K., & Zaltman, G. (1981). Complainers and Noncomplainers Revisited : Another Look At the Data. *ACR North American Advances*, 08, 83-87. <https://www.acrwebsite.org/volumes/9745/volumes/v08/NA-08/full>
- Grosso, M., Castaldo, S., Li, H. A., & Larivière, B. (2020). What information do shoppers share? The effect of personnel-, retailer-, and country-trust on willingness to share information. *Journal of Retailing*, 96(4), 524-547.
- Gurău, C., & Ranchhod, A. (2009). Consumer privacy issues in mobile commerce : A comparative study of British, French and Romanian consumers. *Journal of Consumer Marketing*, 26(7), 496-507. <https://doi.org/10.1108/07363760911001556>
- Gutman, J. (1982). A means-end chain model based on consumer categorization processes. *Journal of marketing*, 46(2), 60-72.
- Gyung Kim, M., Wang, C., & Mattila, A. S. (2010). The relationship between consumer complaining behavior and service recovery : An integrative review. *International Journal of Contemporary Hospitality Management*, 22(7), 975-991. <https://doi.org/10.1108/09596111011066635>
- Håkanson, L., & Ambos, B. (2010). The antecedents of psychic distance. *Journal of International Management*, 16(3), 195-210. <https://doi.org/10.1016/j.intman.2010.06.001>
- Hall, E. T. (1976). *Beyond culture*. Garden City, NJ; 2.
- Hall, E. T. (1959). *The Silent Language*. Greenwich, Connecticut: Fawcett Publications.
- Hallam, C., & Zanella, G. (2017). Online self-disclosure : The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217-227. <https://doi.org/10.1016/j.chb.2016.11.033>

- Hanel, P. H. P., Litzellachner, L. F., & Maio, G. R. (2018). An Empirical Comparison of Human Value Models. *Frontiers in Psychology*, 9, 1643. <https://doi.org/10.3389/fpsyg.2018.01643>
- Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. L. (2007). Overcoming Online Information Privacy Concerns : An Information-Processing Theory Approach. *Journal of Management Information Systems*, 24(2), 13-42. <https://doi.org/10.2753/MIS0742-1222240202>
- Hansen, S. W., Powers, T. L., & Swan, J. E. (1997). Modeling Industrial Buyer Complaints : Implications for Satisfying and Saving Customers. *Journal of Marketing Theory and Practice*, 5(4), 12-22.
- Harmeling, C. M., Moffett, J. W., Arnold, M. J., & Carlson, B. D. (2017). Toward a theory of customer engagement marketing. *Journal of the Academy of Marketing Science*, 45(3), 312-335. <https://doi.org/10.1007/s11747-016-0509-2>
- Hartley, N., & Green, T. (2017). Consumer construal of separation in virtual services. *Journal of Service Theory and Practice*, 27(2), 358-383. <https://doi.org/10.1108/JSTP-05-2015-0118>
- Heidegger, M. (1927). *Être et Temps*. Gallimard.
- Heine, S. J., Lehman, D. R., Markus, H. R., & Kitayama, S. (1999). Is there a universal need for positive self-regard? *Psychological Review*, 106(4), 766-794.
- Heinich, N. (2017). *Des valeurs. Une approche sociologique*. Gallimard.
- Henthorne, T. L., Williams, A. J., & George, B. P. (2018). Cross-cultural consumer complaining behavior in service industries : a three-nation study across the African diaspora. *Journal of Marketing Theory and Practice*, 26(4), 431-446. <https://doi.org/10.1080/10696679.2018.1488220>
- Hirschman, A. O. (1970). *Exit, Voice, and Loyalty : Responses to Decline in Firms, Organizations, and States*. Harvard University Press.
- Hirschman, A. O. (1998). *Crossing boundaries : Selected writings*. Princeton University Press.
- Hirshleifer, J. (1980). Privacy: Its origin, function, and future. *The Journal of Legal Studies*, 9(4), 649-664.
- Hofstede, G. (1984). *Culture's Consequences : International Differences in Work-Related Values*. SAGE.
- Hofstede, G. (1991). *Cultures and Organizations : Software of the mind*. McGraw-Hill.
- Hofstede, G. (2001). *Culture's Consequences : Comparing Values, Behaviors, Institutions and Organizations Across Nations*. SAGE Publications.
- Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations : Software of the mind ; intercultural cooperation and its importance for survival* (Rev. and expanded 3. ed). McGraw-Hill; 2.
- Hofstede, G., & Minkov, M. (2010). Long- versus short-term orientation : New perspectives. *Asia Pacific Business Review*, 16(4), 493-504. <https://doi.org/10.1080/13602381003637609>
- Holbrook, M. B. (1994). Ethics in Consumer Research : An Overview and Prospectus. *ACR North American Advances*, 21, 566-571. <https://www.acrwebsite.org/volumes/5983/volumes/v21/NA-21/full>
- Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns : An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, 37(1), 275-298.
- Hong, Y., Morris, M. W., Chiu, C., & Benet-Martínez, V. (2000). Multicultural minds : A dynamic constructivist approach to culture and cognition. *American Psychologist*, 55(7), 709-720. <https://doi.org/10.1037//0003-066X.55.7.709>
- Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Available at SSRN 1589864.
- Hoult, T. F. (1969). *Dictionary of modern sociology*. Littlefield, Adams.
- House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). *Culture, Leadership and Organizations : The GLOBE Study of 62 Societies*. SAGE.
- Huang, J.-H., Huang, C.-T., & Wu, S. (1996). National character and response to unsatisfactory hotel service. *International Journal of Hospitality Management*, 15(3), 229-243. [https://doi.org/10.1016/S0278-4319\(96\)00009-6](https://doi.org/10.1016/S0278-4319(96)00009-6)

- Huff, L., & Kelley, L. (2003). Levels of Organizational Trust in Individualist Versus Collectivist Societies : A Seven-Nation Study. *Organization Science*, 14(1), 81-90.
<https://doi.org/10.1287/orsc.14.1.81.12807>
- Imm Ng, S., Anne Lee, J., & Soutar, G. N. (2007). Are Hofstede's and Schwartz's value frameworks congruent? *International Marketing Review*, 24(2), 164-180.
<https://doi.org/10.1108/02651330710741802>
- Inglehart, R. (2018). *Cultural Evolution : People's Motivations are Changing, and Reshaping the World*. Cambridge University Press.
- Inglehart, R., & Baker, W. E. (2000). Modernization, Cultural Change, and the Persistence of Traditional Values. *American Sociological Review*, 65(1), 19-51.
<https://doi.org/10.2307/2657288>
- Inglehart, R., & Carballo, M. (1997). Does Latin America Exist? (And Is There a Confucian Culture?): A Global Analysis of Cross-Cultural Differences. *PS: Political Science and Politics*, 30(1), 34-47. 2. <https://doi.org/10.2307/420668>
- Inglehart, R., & Welzel, C. (2005). *Modernization, cultural change, and democracy : The human development sequence*. Cambridge University Press.
- Inglehart, R., & Welzel, C. (2010). Changing Mass Priorities : The Link between Modernization and Democracy. *Perspectives on Politics*, 8(02), 551-567.
<https://doi.org/10.1017/s1537592710001258>
- Jackson, V., Stoel, L., & Brantley, A. (2011). Mall attributes and shopping value : Differences by gender and generational cohort. *Journal of retailing and consumer services*, 18(1), 1-9.
- Jacoby, J., & Jaccard, J. J. (1981). The sources, meaning, and validity of consumer complaint behavior : A psychological analysis. *Journal of Retailing*, 57(3), 4-24.
- Jahandideh, B., Golmohammadi, A., Meng, F., O'Gorman, K. D., & Taheri, B. (2014). Cross-cultural comparison of Chinese and Arab consumer complaint behavior in the hotel context. *International Journal of Hospitality Management*, 41, 67-76.
<https://doi.org/10.1016/j.ijhm.2014.04.011>
- James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs) : Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management*, 54(7), 851-865.
<https://doi.org/10.1016/j.im.2017.01.001>
- Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior : Evidence from a Multichannel Retailer. *Journal of Marketing*, 82(2), 85-105. <https://doi.org/10.1509/jm.16.0124>
- Jasper, C. R., & Waldhart, P. (2013). Internet and distance channel use and European consumer complaint behavior. *The International Review of Retail, Distribution and Consumer Research*, 23(2), 137-151.
- Johnson, G., Shriver, S., & Goldberg, S. (2022). Privacy & market concentration: Intended & unintended consequences of the GDPR. *Available at SSRN 3477686*.
- Johnson, M. P., & Schaltegger, S. (2020). Entrepreneurship for Sustainable Development : A Review and Multilevel Causal Mechanism Framework. *Entrepreneurship Theory and Practice*, 44(6), 1141-1173. <https://doi.org/10.1177/1042258719885368>
- Jones, M. L. (2007, 24-26 June). Hofstede—Culturally questionable?. *Oxford University Business & Economics Conference*.
- Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009). Everyday life, online : US college students' use of the Internet. *First Monday*.
- Kaasa, A. (2021). Merging Hofstede, Schwartz, and Inglehart into a Single System. *Journal of Cross-Cultural Psychology*, 52(4), 339-353. <https://doi.org/10.1177/00220221211011244>
- Kahle, L. R., & Valette-Florence, P. (2012). *Marketplace lifestyles in an age of social media : Theory and methods*. M.E. Sharpe.
- Kahneman, D., & Tversky, A. (1979). Prospect Theory : An Analysis of Decision under Risk. *Econometrica*, 47(2), 263-292.
- Kapferer, J.-N., & Valette-Florence, P. (2019). How self-success drives luxury demand : An integrated model of luxury growth and country comparisons. *Journal of Business Research*, 102, 273-287. <https://doi.org/10.1016/j.jbusres.2019.02.002>

- Kardiner, A. (1939). *The individual and his society : The psychodynamics of primitive social organization* (p. xxvi, 503). Columbia Univ. Press.
- Karunakaran, S., Thomas, K., Bursztein, E., & Comanescu, O. (2018, June). Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. In *SOUPS@USENIX Security Symposium* (pp. 217-234).
- Keaveney, S. M. (1995). Customer Switching Behavior in Service Industries : An Exploratory Study. *Journal of Marketing*, 59(2), 71-82. <https://doi.org/10.2307/1252074>
- Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management : an integrated risk model. *Information & Management*, 58(1), 103392. <https://doi.org/10.1016/j.im.2020.103392>
- Kim, D. H., Sung, Y., & Drumwright, M. (2018). 'Where I come from' determines, 'how I construe my future' : The fit effect of culture, temporal distance, and construal level. *International Journal of Advertising*, 37(2), 270-288. <https://doi.org/10.1080/02650487.2016.1238661>
- Kim, D. H., Sung, Y. H., Lee, S. Y., Choi, D., & Sung, Y. (2016). Are you on Timeline or News Feed? The roles of Facebook pages and construal level in increasing ad effectiveness. *Computers in Human Behavior*, 57, 312-320. <https://doi.org/10.1016/j.chb.2015.12.031>
- Kivetz, Y., & Tyler, T. R. (2007). Tomorrow I'll be me : The effect of time perspective on the activation of idealistic versus pragmatic selves. *Organizational Behavior and Human Decision Processes*, 102(2), 193-211. <https://doi.org/10.1016/j.obhdp.2006.07.002>
- Kluckhohn, C. E., Murray, H. A., & Schneider, D. M. (1953). *Personality in nature, society, and culture* (2nd ed.). Knopf.
- Kluckhohn, F. R., & Strodtbeck, F. L. (1961). *Variations in value orientations* (p. xiv, 450). Row, Peterson.
- Knox, G., & van Oest, R. (2014). Customer Complaints and Recovery Effectiveness : A Customer Base Approach. *Journal of Marketing*, 78(5), 42-57.
- Kolm, S. C. (2002). *Justice and equity*. MIT Press.
- Kogut, B. and Singh, H. (1988), The effect of national culture on the choice of entry mode, *Journal of International Business Studies*, 19(3), 411-32.
- Koops, B.-J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L.*, 38(2), 483-575.
- Krafft, M., Kumar, V., Harmeling, C., Singh, S., Zhu, T., Chen, J., Duncan, T., Fortin, W., & Rosa, E. (2021). Insight is power : Understanding the terms of the consumer-firm data exchange. *Journal of Retailing*, 97(1), 133-149. <https://doi.org/10.1016/j.jretai.2020.11.001>
- Krasnova, H., & Veltri, N. F. (2010). Privacy Calculus on Social Networking Sites : Explorative Evidence from Germany and USA. *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010 (pp. 1-10). <https://doi.org/10.1109/HICSS.2010.307>
- Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites : The Role of Culture: Intercultural Dynamics of Privacy Calculus. *Business & Information Systems Engineering*, 4(3), 127-135. <https://doi.org/10.1007/s12599-012-0216-6>
- Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, 38(11), 1134-1145. <https://doi.org/10.1016/j.telpol.2014.10.002>
- Kuhlmann, S., & Rip, A. (2019). Next generation science policy and Grand Challenges. In D. Simon, S. Kuhlmann, J. Stamm, & W. Canzler, *Handbook on Science and Public Policy* (pp. 12-25). Edward Elgar Publishing. <https://doi.org/10.4337/9781784715946.00009>
- Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. University of Chicago Press.
- Kumaraguru, P., & Cranor, L. F. (2005). Privacy Indexes : A Survey of Westin's Studies. 22.
- Labrecque, L. I. (2021). When data security goes wrong : Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, 135, 559-571.
- Ladwein, R. (2003). *Le comportement du consommateur et de l'acheteur*. Pris : Economica.
- Lapidus, R. S., & Pinkerton, L. (1995). Customer complaint situations : An equity theory perspective. *Psychology & Marketing*, 12(2), 105-122. <https://doi.org/10.1002/mar.4220120203>

- Larasati, Z. W., Yuda, T. K., & Syafa'at, A. R. (2022). Digital welfare state and problem arising : An exploration and future research agenda. *International Journal of Sociology and Social Policy*, (ahead-of-print). <https://doi.org/10.1108/IJSSP-05-2022-0122>
- Latour, B., & Woolgar, S. (1979). *La vie de laboratoire*. Éditions La Découverte.
- Lazarus, R. S. (1966). *Psychological stress and the coping process*. New York: McGraw-Hill.
- Lazarus, R. S. (1991). Progress on a cognitive-motivational-relational theory of emotion. *American psychologist*, 46(8), 819-834.
- Lee, E.-J., & Park, J. K. (2009). Online service personalization for apparel shopping. *Journal of Retailing and Consumer Services*, 16(2), 83-91. <https://doi.org/10.1016/j.jretconser.2008.10.003>
- Lee, S., & Cude, B. J. (2012). Consumer complaint channel choice in online and offline purchases : Consumer complaint channels. *International Journal of Consumer Studies*, 36(1), 90-96. <https://doi.org/10.1111/j.1470-6431.2010.00992.x>
- Lenartowicz, T., & Roth, K. (1999). A Framework for Culture Assessment. *Journal of International Business Studies*, 30(4), 781-798.
- Li, L., Chang, Y., Lee, K. Y., & Yang, S.-B. (2020). Linking Privacy Concerns for Traceable Information and Information Privacy Protective Responses on Electric Scooter Sharing Platforms. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020 (pp. 851-857).
- Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns : Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(28), 453-496. <https://doi.org/10.17705/1CAIS.02828>
- Li, Y. (2012). Theories in online information privacy research : A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481. <https://doi.org/10.1016/j.dss.2012.06.010>
- Li, Y., Kobsa, A., Knijnenburg, B. P., & Nguyen, M.-H. C. (2017). Cross-Cultural Privacy Prediction. *Proceedings on Privacy Enhancing Technologies*, 113-132.
- Li, Y., Rho, E. H. R., & Kobsa, A. (2022). Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology*, 41(3), 655-677. <https://doi.org/10.1080/0144929X.2020.1831608>
- Liljenstrom, H., & Svedin, U. (2005). *Micro Meso Macro : Addressing Complex Systems Couplings*. World Scientific.
- Lind, E. A., & Earley, P. C. (1992). Procedural Justice and Culture. *International Journal of Psychology*, 27(2), 227-242. <https://doi.org/10.1080/00207599208246877>
- Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*. Springer Science & Business Media.
- Lippert, S. K., & Michael Swiercz, P. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science*, 31(5), 340-353. <https://doi.org/10.1177/0165551505055399>
- Liu, B. S.-C., Furrer, O., & Sudharshan, D. (2001). The Relationships between Culture and Behavioral Intentions toward Services. *Journal of Service Research*, 4(2), 118-129. 0.3. <https://doi.org/10.1177/109467050142004>
- Liu, R. R., & McClure, P. (2001). Recognizing cross-cultural differences in consumer complaint behavior and intentions : An empirical examination. *Journal of Consumer Marketing*, 18(1), 54-75. 0.3. <https://doi.org/10.1108/07363760110365813>
- Liu, B., Pavlou, P. A., & Cheng, X. (2021). Achieving a Balance Between Privacy Protection and Data Collection : A Field Experimental Examination of a Theory-Driven Information Technology Solution. *Information Systems Research*, 33(1), 203-223. <https://doi.org/10.1287/isre.2021.1045>
- Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites : A cross-cultural comparison. *Information & Management*, 55(8), 1005-1023. <https://doi.org/10.1016/j.im.2018.05.006>
- Livian, Y. (2011). Pour en finir avec Hofstede. *Conference Atlas-AFMI, Association Francophone de Management International*.

- Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies : The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems*, 27(4), 163-200. <https://doi.org/10.2753/MIS0742-1222270406>
- Lunnay, B., Ward, P., & Borlagdan, J. (2011). The practise and practice of Bourdieu : The application of social theory to youth alcohol research. *International Journal of Drug Policy*, 22(6), 428-436. <https://doi.org/10.1016/j.drugpo.2011.07.013>
- Lutz, C., & Strathoff, P. (2014). Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2425132>
- Madan, S., Savani, K., & Katsikeas, C. S. (2022). Privacy please : Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, 1-24. <https://doi.org/10.1057/s41267-022-00519-5>
- Maio, G. R., Olson, J. M., Bernard, M. M., & Luke, M. A. (2006). Ideologies, Values, Attitudes, and Behavior. In J. Delamater, *Handbook of Social Psychology* (pp. 283-308). Springer US. https://doi.org/10.1007/0-387-36921-X_12
- Maisonneuve, J. (2017). *La psychologie sociale*. «Que sais-je?» n° 458. Que sais-je.
- Malhotra, A., & Kubowicz Malhotra, C. (2011). Evaluating Customer Information Breaches as Service Failures : An Event Study Approach. *Journal of Service Research*, 14(1), 44-59. <https://doi.org/10.1177/1094670510383409>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC) : The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.
- Maller, C. (2012). Using social practice theory to understand everyday life in a master-planned estate : Outcomes for health and wellbeing. *The Annual Conference of the Australian Sociological Association: Emerging and Enduring Inequalities, Refereed Conference Proceedings*, 1-16.
- Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44. <https://doi.org/10.1016/j.chb.2018.01.028>
- Margulis, S. T. (1977). Conceptions of Privacy : Current Status and Next Steps. *Journal of Social Issues*, 33(3), 5-21. <https://doi.org/10.1111/j.1540-4560.1977.tb01879.x>
- Mariani, M., Di Fatta, G., & Di Felice, M. (2019). Understanding Customer Satisfaction With Services by Leveraging Big Data : The Role of Services Attributes and Consumers' Cultural Background. *IEEE Access*, 7, 8195-8208. <https://doi.org/10.1109/ACCESS.2018.2887300>
- Mariani, M., Perez-Vega, R., & Wirtz, J. (2022). AI in marketing, consumer research and psychology : A systematic literature review and research agenda. *Psychology & Marketing*, 39(4), 755-776. <https://doi.org/10.1002/mar.21619>
- Markus, H. R., & Kitayama, S. (1990). Culture and the Self : Implications for Cognition, Emotion, and Motivation. *Psychological Review*, 98(2), 224-253.
- Martin, K. . (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*, 111(4), 519-539
- Martin, K. (2016). Understanding privacy online : Development of a social contract approach to privacy. *Journal of business ethics*, 137(3), 551-569.
- Martin, K. (2018). The penalty for privacy violations : How privacy violations impact trust online. *Journal of Business Research*, 82, 103-116. <https://doi.org/10.1016/j.jbusres.2017.08.034>
- Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Colum. Sci. & Tech. L. Rev.*, 18, 176.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.
- Martin, K. D., Borah, A., & Scott, M. L. (2021). The Journal of Public Policy & Marketing at 40 : Celebrating History and Impact. *Journal of Public Policy & Marketing*, 40(3), 301-321. <https://doi.org/10.1177/07439156211018689>
- Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., ... & Weaven, S. K. (2020). Data privacy in retail. *Journal of Retailing*, 96(4), 474-489. <https://doi.org/10.1016/j.jretai.2020.08.003>

- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155. <https://doi.org/10.1007/s11747-016-0495-4>
- Martin, K. D., & Palmatier, R. W. (2020). Data Privacy in Retail : Navigating Tensions and Directing Future Research. *Journal of Retailing*, 96(4), 449-457. <https://doi.org/10.1016/j.jretai.2020.10.002>
- Maslow, A. H. (1954). *Motivation and Personality*. New York-Harper and Row.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370-396. <https://doi.org/10.1037/h0054346>
- Matsumoto, D. (2007). Culture, context, and behavior. *Journal of personality*, 75(6), 1285-1319.
- Mattelart, A. (2010). *Diversité culturelle et mondialisation*. La Découverte.
- Mauss, M., & Durkheim. (1913). Note sur la notion de civilisation. *Année sociologique*, 12, 451-455.
- Maynard, M. L., & Taylor, C. R. (1996). A comparative analysis of Japanese and U.S. attitudes toward direct marketing. *Journal of Direct Marketing*, 10(1), 34-44. 0.1.
- McCort, D. J., & Malhotra, N. K. (1993). Culture and Consumer Behavior : Toward an Understanding of Cross-Cultural Consumer Behavior in International Marketing. *Journal of International Consumer Marketing*, 6(2), 91-127. https://doi.org/10.1300/J046v06n02_07
- McGuire, W. J. (1964). Some Contemporary Approaches11, In L. Berkowitz (Éd.), *Advances in Experimental Social Psychology*, 1 (pp. 191-229). Academic Press. [https://doi.org/10.1016/S0065-2601\(08\)60052-0](https://doi.org/10.1016/S0065-2601(08)60052-0)
- McSweeney, B. (2002). Hofstede's model of national cultural differences and their consequences : A triumph of faith – a failure of analysis. *Human Relations*, 55(1), 89-118.
- Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12), 65-74. <https://doi.org/10.1145/219663.219683>
- Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy : Corporate Management and National Regulation. *Organization Science*, 11(1), 35-57.
- Miller, N. E. (1944). Experimental studies of conflict.
- Mills, J. L., & Harclerode, K. (2018). *Privacy Mass Intrusion and the Modern Data Breach*. Florida Law Review.
- Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy : A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing*, 19(1), 1-6. <https://doi.org/10.1509/jppm.19.1.1.16934>
- Miltgen, C. L. (2009). Propension à fournir des données personnelles mensongères sur Internet : Une étude exploratoire. *Systèmes d'information & management*, 14(3), 9-42. <https://doi.org/10.3917/sim.093.0009>
- Miltgen, C. L. (2010). Dévoilement de données personnelles et contreparties attendues en e-commerce : Une approche typologique et interculturelle. *Systèmes d'information & management*, 15(4), 45-91. <https://doi.org/10.3917/sim.104.0045>
- Miltgen, C. L., Henseler, J., Gelhard, C., & Popović, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*, 69(10), 4659-4666.
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns : A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103-125. 0.1. <https://doi.org/10.1057/ejis.2013.17>
- Miltgen, C. L., & Smith, H. J. (2019). Falsifying and withholding : Exploring individuals' contextual privacy-related decision-making. *Information & Management*, 56(5), 696-717. <https://doi.org/10.1016/j.im.2018.11.004>
- Minkov, M. (2018). A revision of Hofstede's model of national culture : Old evidence and new data from 56 countries. *Cross Cultural & Strategic Management*, 25(2), 231-256. <https://doi.org/10.1108/CCSM-03-2017-0033>
- Moalla, E. (2016). Quelle mesure pour la culture nationale ? Hofstede vs Schwartz vs Globe. *Management international*, 20, 26-37. <https://doi.org/10.7202/1063703ar>
- Mooradian, T. A., & Olver, J. M. (1997). "I can't get no satisfaction:" The impact of personality and emotion on postpurchase processes. *Psychology & Marketing*, 14(4), 379-393.

- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research*, 15(1), 76-98.
- Moscarola, J. (2018). Chapitre 9. Analyse de données textuelles, lexicales et sémantiques. In Moscarola, J., *Faire parler les données* (pp. 191-217). EMS Éditions.
- Muk, A. (2007). Cultural influences on adoption of SMS advertising : A study of American and Taiwanese consumers. *Journal of Targeting, Measurement and Analysis for Marketing*, 16(1), 39-47. <https://doi.org/10.1057/palgrave.jt.5750062>
- Murphy-Berman, V., & Berman, J. (1998). Cross-Cultural Differences in Perceptions of Distributive Justice : A comparison of Hong Kong and Indonesia. *Journal of Cross-Cultural Psychology*, 33(2), 157-170. <https://doi.org/10.1027//1016-9040.3.1.76>
- Ngai, E. W. T., Heung, V. C. S., Wong, Y. H., & Chan, F. K. Y. (2007). Consumer complaint behaviour of Asians and non-Asians about hotel services : An empirical analysis. *European Journal of Marketing*, 41(11/12), 1375-1391. <https://doi.org/10.1108/03090560710821224>
- N'Goala, G., Pez-Pérard, V., & Prim-Allaz, I. (2019). *Stratégie clients augmentée : La relation client réinventée à l'ère du tout-numérique*. ISTE Group.
- Nguyen, T. N., Lobo, A., & Greenland, S. (2017). The influence of cultural values on green purchase behaviour. *Marketing Intelligence & Planning*, 35(3), 377-396. <https://doi.org/10.1108/MIP-08-2016-0131>
- Nisan, M. (1972). Dimension of time in relation to choose behavior and achievement orientation. *Journal of Personality and Social Psychology*, 21(2), 175-182.
- Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 41.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1), 100-126.
- Nova, N., Miyake, K., Chiu, W., & Kwon, N. (2012). *Curious Rituals*. NFL press. <https://hal.science/hal-02937719>
- Ohlhausen, M. K. (2014). Privacy Challenges and Opportunities : The Role of the Federal Trade Commission. *Journal of Public Policy & Marketing*, 33(1), 4-9.
- Ortner, S. B. (2006). *Anthropology and Social Theory : Culture, Power, and the Acting Subject*. Duke University Press.
- Oyserman, D. (2006). High Power, Low Power, and Equality : Culture Beyond Individualism and Collectivism. *Journal of Consumer Psychology*, 16(4), 352-356. https://doi.org/10.1207/s15327663jcp1604_6
- Oyserman, D. (2012). Values : Psychological Perspectives. *International Encyclopedia of the Social and Behavioral Sciences*, 16150-16153. <https://doi.org/10.1016/B0-08-043076-7/01735-6>
- Oyserman, D., Coon, H. M., & Kemmelmeier, M. (2002). Rethinking individualism and collectivism : Evaluation of theoretical assumptions and meta-analyses. *Psychological Bulletin*, 128(1), 3-72. <https://doi.org/10.1037//0033-2909.128.1.3>
- Papaoikonomou, E., Valverde, M., & Ryan, G. (2012). Articulating the Meanings of Collective Experiences of Ethical Consumption. *Journal of Business Ethics*, 110(1), 15-32. <https://doi.org/10.1007/s10551-011-1144-y>
- Parguel, B., Lunardo, R., & Benoit-Moreau, F. (2017). Sustainability of the sharing economy in question : When second-hand peer-to-peer platforms stimulate indulgent consumption. *Technological Forecasting and Social Change*, 125, 48-57. <https://doi.org/10.1016/j.techfore.2017.03.029>
- Parguel, B., Monnot, E., Reniou, F., & Benoit-Moreau, F. (2018). Les finalités sociétales dans la recherche francophone en marketing : Une lecture historique et critique. *Revue Française de Gestion*, 44(276), 11-31. <https://doi.org/10.3166/rfg.2018.00283>
- Park, C., Jun, J., & Lee, T. (2015). Consumer characteristics and the use of social networking sites : A comparison between Korea and the US. *International Marketing Review*, 32(3/4), 414-437. <https://doi.org/10.1108/IMR-09-2013-0213>
- Pasquale, F. (2015). *The Black Box Society*. Harvard University Press; 1.

- Pasquier, D. (2018). *L'Internet des familles modestes : Enquête dans la France rurale*. Presses des Mines via OpenEdition.
- Pavlou, P. A. (2011). State of the Information Privacy Literature : Where are We Now And Where Should We Go? *MIS Quarterly*, 35(4), 977-988. <https://doi.org/10.2307/41409969>
- Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of environmental psychology*, 17(2), 147-156.
- Peng, K., & Nisbett, R. E. (1999). Culture, dialectics, and reasoning about contradiction. *American psychologist*, 54(9), 741-787.
- Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 65, 409-419.
- Petrescu, M., Krishen, A., & Bui, M. (2020). The internet of everything : Implications of marketing analytics from a consumer policy perspective. *Journal of Consumer Marketing*, 37(6), 675-686. <https://doi.org/10.1108/JCM-02-2019-3080>
- Popper, K. R. (1959). The propensity interpretation of probability. *The British journal for the philosophy of science*, 10(37), 25-42.
- Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model : The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems*, 19(2), 181-195. <https://doi.org/10.1057/ejis.2010.15>
- Posner, R. A. (1978). Economic Theory of Privacy. *Regulation*, 2, 19.
- Prime, N., & Usunier, J.-C. (2012). *Marketing international : Marchés, cultures et organisations*. Pearson education.
- Pueschel, J., Parguel, B., & Chamaret, C. (2021). Talking about my generation: comment les valeurs façonnent la consommation de luxe. *Recherche et Applications en Marketing (French Edition)*, 36(2), 24-44.
- Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and Artificial Intelligence : An Experiential Perspective. *Journal of Marketing*, 85(1), 131-151. <https://doi.org/10.1177/0022242920953847>
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies : Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299-1323. <https://doi.org/10.1007/s11747-022-00845-y>
- Rajavi, K., Kushwaha, T., & Steenkamp, J.-B. E. M. (2019). In Brands We Trust? A Multicategory, Multicountry Investigation of Sensitivity of Consumers' Trust in Brands to Marketing-Mix Activities. *Journal of Consumer Research*, 46(4), 651-670. <https://doi.org/10.1093/jcr/ucz026>
- Rasoulilian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2017). Service crisis recovery and firm performance : Insights from information breach announcements. *Journal of the Academy of Marketing Science*, 45(6), 789-806. <https://doi.org/10.1007/s11747-017-0543-8>
- Rasoulilian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2021). The Effects of Service Crises and Recovery Resources on Market Reactions : An Event Study Analysis on Data Breach Announcements. *Journal of Service Research*, 26(1), 44-63. <https://doi.org/10.1177/10946705211036944>
- Rawls, J. (1971). *A theory of justice*. The Belknap.
- Rejikumar, G., Gopikumar, V., Dinesh, K. S., Asokan-Ajitha, A., & Jose, A. (2021). Privacy breach perceptions and litigation intentions: Evidence from e-commerce customers. *IIMB Management Review*, 33(4), 322-336.
- Renan, E. (1882). *Qu'est-ce qu'une Nation?*
- Reynolds, T. J., & Gutman, J. (1988). Laddering theory, method, analysis, and interpretation. *Journal of advertising research*, 28(1), 11-31.
- Rip, A., & Kemp, R. (1998). Technological change. *Human choice and climate change*, 2(2), 327-399.
- Ro, H. (2015). Customer Dissatisfaction Responses to Restaurant Service Failures : Insights Into Noncomplainers From a Relational Perspective. *Journal of Hospitality Marketing & Management*, 24(4), 435-456. <https://doi.org/10.1080/19368623.2014.910481>
- Robson, C. (2002). *Real world research : A resource for social scientists and practitioner-researchers (2nd ed)*. Blackwell Publishers.

- Rochelandet, F. (2010). *Économie des données personnelles et de la vie privée*. La Découverte.
- Rokeach, M. (1973). *The Nature of Human Values*. Free Press.
- Rokeach, M. (1979). Some unresolved issues in theories of beliefs, attitudes, and values. *Nebraska Symposium on Motivation*, 27, 261-304.
- Rokeach, M. (2008). *Understanding Human Values*. Simon and Schuster.
- Romanosky, S., Hoffman, D., & Acquisti, A. (2013). Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, 11(1), 74-104.
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? : Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management*, 30(2), 256-286. <https://doi.org/10.1002/pam.20567>
- Ronteltap, A., Sijtsema, S. J., Dagevos, H., & de Winter, M. A. (2012). Construal levels of healthy eating. Exploring consumers' interpretation of health in the food context. *Appetite*, 59(2), 333-340. <https://doi.org/10.1016/j.appet.2012.05.023>
- Ryan, A. B. (2006). Post-positivist approaches to research. *Researching and Writing your Thesis: a guide for postgraduate students*, 12-26.
- Sabadie, W., Prim-Allaz, I., & Llosa, S. (2006). Contribution des éléments de gestion des réclamations à la satisfaction : Les apports de la théorie de la justice. *Recherche et Applications En Marketing*, 21(3), 47-64. <https://doi.org/10.1177/076737010602100303>
- Craig, C.S., & Douglas, S. P. (2006). Beyond national culture : Implications of cultural dynamics for consumer research. *International Marketing Review*, 23(3), 322-342. <https://doi.org/10.1108/02651330610670479>
- Sapir, E. (1921). Language, race and culture. In *Language : An introduction to the study of speech* (pp. 207-220). Harcourt Brace & Company. <https://doi.org/10.1037/13026-010>
- Schatzki, T. R. (1996). *Social Practices : A Wittgensteinian Approach to Human Activity and the Social*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511527470>
- Schaufeli, W. B. (2013). What is engagement? In Truss, C., Alfes, K., Delbridge, R., Shantz, A., & Soane, E. *Employee Engagement in Theory and Practice* (pp. 29-49) Routledge.
- Schein, E. H. (1984). Culture as an environmental context for careers. *Journal of Organizational Behavior*, 5(1), 71-81. <https://doi.org/10.1002/job.4030050107>
- Schein, E. H., Costas, J., Kunda, G., Schultz, M., Connolly, T. H., Wright, S., Hofstede, G. J., & Wah, D. W. H. (2015). Opinions : All About Culture. *Journal of Business Anthropology*, 4(1), 106-150. <https://doi.org/10.22439/jba.v4i1.4792>
- Schwartz, B. (1968). The Social Psychology of Privacy. *American Journal of Sociology*, 73(6), 741-752. <https://doi.org/10.1086/224567>
- Schwartz, S. H. (1992). Universals in the Content and Structure of Values : Theoretical Advances and Empirical Tests in 20 Countries. In *Advances in Experimental Social Psychology*, 25 (pp. 1-65). Elsevier. [https://doi.org/10.1016/S0065-2601\(08\)60281-6](https://doi.org/10.1016/S0065-2601(08)60281-6)
- Schwartz, S. H. (1994). Are there universal aspects in the structure and contents of human values? *Journal of social issues*, 50(4), 19-45.
- Schwartz, S. H. (1999). A theory of cultural values and some implications for work. *Applied psychology*, 48(1), 23-47.
- Schwartz, S. H. (2006). Les valeurs de base de la personne : Théorie, mesures et applications. *Revue française de sociologie*, 47(4), 929-968. <https://doi.org/10.3917/rfs.474.0929>
- Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J.-E., Demirutku, K., Dirilen-Gumus, O., & Konty, M. (2012). Refining the theory of basic individual values. *Journal of Personality and Social Psychology*, 103(4), 663-688. <https://doi.org/10.1037/a0029393>
- Shapira, O., Liberman, N., Trope, N., & Rim, S.Y. (2012) Levels of mental construal. In Fiske, S., & McRae, N., *The SAGE Handbook of Social Cognition* (pp. 229-250). Thousand Oaks.
- Sharma, P. (2010). Measuring personal cultural orientations : Scale development and validation. *Journal of the Academy of Marketing Science*, 38(6), 787-806. <https://doi.org/10.1007/s11747-009-0184-7>
- Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining : How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28(3), 37-51.

- Shove, E. (2010). Beyond the ABC : Climate Change Policy and Theories of Social Change. *Environment and Planning. Economy and Space*, 42(6), 1273-1285. <https://doi.org/10.1068/a42282>
- Shove, E. (2011). How the Social Sciences Can Help Climate Change Policy. An Extraordinary Lecture and Accompanying Exhibition. *Performed by members of the social change climate change working party at the British Library, London.*
- Shove, E., & Pantzar, M. (2005). Consumers, Producers and Practices : Understanding the invention and reinvention of Nordic walking. *Journal of Consumer Culture*, 5(1), 43-64. <https://doi.org/10.1177/1469540505049846>
- Shove, E., Pantzar, M., & Watson, M. (2012). *The dynamics of social practice : Everyday life and how it changes*. SAGE.
- Singh, A. S., Zwickle, A., Bruskotter, J. T., & Wilson, R. (2017). The perceived psychological distance of climate change impacts and its influence on support for adaptation policy. *Environmental Science & Policy*, 73, 93-99. <https://doi.org/10.1016/j.envsci.2017.04.011>
- Singh, J. (1988). Consumer Complaint Intentions and Behavior : Definitional and Taxonomical Issues. *Journal of Marketing*, 52(1), 93-107.
- Singh, J. (1990). Voice, exit, and negative word-of-mouth behaviors : An investigation across three service categories. *Journal of the Academy of Marketing Science*, 18(1), 1-15. <https://doi.org/10.1007/BF02729758>
- Siret, I., & Sabadie, W. (2022). Public complaining : A blessing in disguise? Educational calling as a benevolent process that gives consumers voice on brands' social media. *Journal of Business Research*, 150, 476-490. <https://doi.org/10.1016/j.jbusres.2022.05.084>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research : An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989-1016. <https://doi.org/10.2307/41409970>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy : Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167. <https://doi.org/10.2307/249477>
- Soares, A. M., Farhangmehr, M., & Shoham, A. (2007). Hofstede's dimensions of culture in international marketing studies. *Journal of Business Research*, 60(3), 277-284. <https://doi.org/10.1016/j.jbusres.2006.10.018>
- Solove, D. J. (2013). *Privacy Self-Management and the Consent Dilemma*. 126 Harv. L. Rev. 1880.
- Solove, D. J. (2020). The Myth of the Privacy Paradox. *SSRN Electronic Journal*. 1. <https://doi.org/10.2139/ssrn.3536265>
- Solove, D. J., & Hartzog, W. (2022). *Breached! : Why Data Security Law Fails and How to Improve it*. Oxford University Press.
- Son, J.-Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses : A Taxonomy and a Nomological Model. *MIS Quarterly*, 32, 503-529. <https://doi.org/10.2307/25148854>
- Spassova, G., & Lee, A. Y. (2013). Looking into the Future : A Match between Self-View and Temporal Distance. *Journal of Consumer Research*, 40(1), 159-171. <https://doi.org/10.1086/669145>
- Spence, A., Poortinga, W., Butler, C., & Pidgeon, N. F. (2011). Perceptions of climate change and willingness to save energy related to flood experience. *Nature Climate Change*, 1(1), 46-49. <https://doi.org/10.1038/nclimate1059>
- Spence, A., Poortinga, W., & Pidgeon, N. (2012). The Psychological Distance of Climate Change : Psychological Distance of Climate Change. *Risk Analysis*, 32(6), 957-972. <https://doi.org/10.1111/j.1539-6924.2011.01695.x>
- Spranger, E. (1928). *Types of men. The psychology and ethics of personality* (p. xii, 402). Niemeyer.
- Srite, M., & Karahanna, E. (2006). The Role of Espoused National Cultural Values in Technology Acceptance. *MIS Quarterly*, 30(3), 679-704. <https://doi.org/10.2307/25148745>
- Stauss, B., Schmidt, M., & Schoeler, A. (2005). Customer frustration in loyalty programs. *International Journal of Service Industry Management*, 16(3), 229-252.
- Steenkamp, J-B. E. M. (2001). The role of national culture in international marketing research. *International Marketing Review*, 18(1), 30-44. <https://doi.org/10.1108/02651330110381970>

- Steenkamp, J.-B. E. M. (2019). Global Versus Local Consumer Culture : Theory, Measurement, and Future Research Directions. *Journal of International Marketing*, 27(1), 1-19.
<https://doi.org/10.1177/1069031X18811289>
- Steenkamp, J.-B. E. M., & Geyskens, I. (2006). How Country Characteristics Affect the Perceived Value of Web Sites. *Journal of Marketing*, 70(3), 136-150.
<https://doi.org/10.1509/jmkg.70.3.136>
- Stephens, N., & Gwinner, K. P. (1998). Why Don't Some People Complain? A Cognitive-Emotive Process Model of Consumer Complaint Behavior. *Journal of the Academy of Marketing Science*, 26(3), 172-189. <https://doi.org/10.1177/0092070398263001>
- Sykes, C. J. (1999). *The end of privacy : The attack on personal rights at home, at work, on-line, and in court*. St. Martin's Press.
- Ting-toomey, S., & Kurogi, A. (1998). Facework competence in intercultural conflict : An updated face-negotiation theory. *International Journal of Intercultural Relations*, 22(2), 187-225.
[https://doi.org/10.1016/S0147-1767\(98\)00004-2](https://doi.org/10.1016/S0147-1767(98)00004-2)
- Tonnies, F. (1887). *Community and Society*, new ed. 1963, transl. By CP Loomis. New York.
- Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption : An investigation of challenges and expected value. *Information & Management*, 58(3), 103444.
<https://doi.org/10.1016/j.im.2021.103444>
- Travers, M. W. (2015). *Phenomenological foundations of psychological distance* [PhD Thesis. University of Colorado at Boulder].
- Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, 3(1), 2056305116688035. <https://doi.org/10.1177/2056305116688035>
- Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert, *Reforming European Data Protection Law* (pp. 333-365). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14
- Triandis, H. C. (1993). Collectivism and Individualism as Cultural Syndromes. *Cross-Cultural Research*, 27(3-4), 155-180. <https://doi.org/10.1177/106939719302700301>
- Triandis, H. C. (1996). The psychological measurement of cultural syndromes. *American Psychologist*, 51(4), 407-415. <https://doi.org/10.1037/0003-066X.51.4.407>
- Triandis, H. C., Leung, K., Villareal, M. J., & Clack, F. I. (1985). Allocentric versus idiocentric tendencies: Convergent and discriminant validation. *Journal of Research in personality*, 19(4), 395-415.
- Trompenaars, F. (1996). Resolving International Conflict : Culture and Business Strategy. *Business Strategy Review*, 7(3), 51-68. <https://doi.org/10.1111/j.1467-8616.1996.tb00132.x>
- Trompenaars, F., & Hampden-Turner, C. (1998). *Understanding cultural diversity in business*. Irwin, London, England.
- Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, 117(2), 440-463. <https://doi.org/10.1037/a0018963>
- Tsoi, H. K., & Chen, L. (2011, October). From privacy concern to uses of social network sites: A cultural comparison via user survey. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (pp. 457-464). IEEE.
- Turner, S. P. (1994). *The Social Theory of Practices : Tradition, Tacit Knowledge, and Presuppositions*. University of Chicago Press.
- Tylor, E. B. (1871). *Primitive Culture : Researches Into the Development of Mythology, Philosophy, Religion, Art and Custom* (Vol.2). J. Murray.
- Urien, B. (2002). Validation d'une échelle de mesure d'une nouvelle dimension temporelle en comportement du consommateur: l'anxiété face à l'avenir. *Revue française du marketing*, 189(190), 77-91.
- Uslaner, E. M. (2008). Where You Stand Depends Upon Where Your Grandparents Sat : The Inheritability of Generalized Trust. *Public Opinion Quarterly*, 72(4), 725-740.
<https://doi.org/10.1093/poq/nfn058>

- Valette-Florence, P. (1986). Les démarches de styles de vie : Concepts, champs d'investigation et problèmes actuels. *Recherche et Applications en Marketing*, 1(2), 41-58.
- Valette-Florence, P. (1994). Introduction à l'analyse des chaînages cognitifs. *Recherche et Applications en Marketing*, 9(1), 93-117.
- Valette-Florence, P., Ferrandi, J.-M., & Roehrich, G. (2003). Apport des chaînages cognitifs à la segmentation des marchés. *Décisions Marketing*, 31-43.
- Valette-Florence, P., & Rapacchi, B. (1991). A cross-cultural means-end chain analysis of perfume purchases. *Proceedings of the Third Symposium on Cross-Cultural Consumer Behavior and Business Studies*, 161-173.
- Vallacher, R. R., & Wegner, D. M. (1989). Levels of Personal Agency : Individual Variation in Action Identification. *Journal of Personality and Social Psychology*, 57(4), 660-671.
- Vallet, C. (2012). Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs. *Droit et société*, 1(80), 163-188. <https://doi.org/10.3917/drs.080.0163>
- Valor, C., Díaz, E. M., & Merino, A. (2017). The discourse of the consumer resistance movement : Adversarial and prognostic framings through the lens of power. *Journal of Macromarketing*, 37(1), 72-84.
- Van de Vijver, F., & Tanzer, N. K. (1997). Bias and equivalence in cross-cultural assessment. *European review of applied psychology*, 47(4), 263-279.
- Van Lange, P. A. M., De Bruin, E. M. N., Otten, W., and Joireman, J. A. (1997). Development of prosocial, individualistic, and competitive orientations: theory and preliminary evidence. *J. Pers. Soc. Psychol.* 73, 733-746. doi: 10.1037/0022- 3514.73.4.733
- Véliz, C. (2020). *Privacy is power : Why and how you should take back control of your data*. Bantam Press.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology : Toward a Unified View. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>
- Walker, B. A., & Olson, J. C. (1991). Means-end chains : Connecting products with self. *Journal of business research*, 22(2), 111-118.
- Wan, L. C. (2013). Culture's impact on consumer complaining responses to embarrassing service failure. *Journal of Business Research*, 66(3), 298-305. <https://doi.org/10.1016/j.jbusres.2011.08.009>
- Warland, R. H., Hermann, R. O. & Willis, J. (1975). Dissatisfied consumers: Who gets upset and who takes action. *Journal of Consumer Affairs*, 9 (2), 148-163.
- Warren, & Brandeis. (1890). *The Right to Privacy*.
- Watkins, H. S., & Liu, R. (1996). Collectivism, Individualism and In-Group Membership : Implications for Consumer Complaining Behaviors in Multicultural Contexts. *Journal of International Consumer Marketing*, 8(3-4), 69-96. https://doi.org/10.1300/J046v08n03_05
- Weber, C. & Jean-Philippe. (2017). La place de l'homme dans les enjeux de cybersécurité. *Stratégique*, 117(4), 83-98. <https://doi.org/10.3917/strat.117.0083>
- Weber, R. (2004). Editor's Comments : The Rhetoric of Positivism versus Interpretivism: A Personal View. *MIS Quarterly*, 28(1), iii-xii. <https://doi.org/10.2307/25148621>
- Webster, F. E. (1975). Determining the Characteristics of the Socially Conscious Consumer. *The Journal of Consumer Research*, 2(3), 188-196.
- Westin, A. F. (1968). *Privacy and freedom*. Washington and Lee Law Review, 25(1), 166.
- Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models : Guidelines and empirical illustration. *MIS quarterly*, 177-195.
- Wiesenfeld, B. M., Reyt, J.-N., Brockner, J., & Trope, Y. (2017). Construal Level Theory in Organizational Research. *Annual Review of Organizational Psychology and Organizational Behavior*, 4(1), 367-400. <https://doi.org/10.1146/annurev-orgpsych-032516-113115>
- Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, 11(2), 378-389.
- Wittgenstein, L. (1958). *Recherches philosophiques*. Gallimard.
- Yang, K. C. C., & Kang, Y. (2015). Exploring Big Data and Privacy in Strategic Communication Campaigns : A Cross-Cultural Study of Mobile Social Media Users' Daily Experiences.

- International Journal of Strategic Communication*, 9(2), 87-101.
<https://doi.org/10.1080/1553118X.2015.1008635>
- Yetiser, B. (2014). Do all roads lead to Rome? The moderating role of culture and age in predicting construal level on machiavellianism. *Yasar Üniversitesi E-Dergisi*, 9(36), 6328-6337.
- Yoo, B., & Donthu, N. (2005). The Effect of Personal Cultural Orientation on Consumer Ethnocentrism : Evaluations and Behaviors of U.S. Consumers Toward Japanese Products. *Journal of International Consumer Marketing*, 18(1-2), 7-44.
- Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns : An analysis of contexts and research constructs. *Information & Management*, 56(4), 570-601. <https://doi.org/10.1016/j.im.2018.10.001>
- Zakaria, N., Stanton, J. M., & Sarkar-Barney, S. T. M. (2003). Designing and implementing culturally-sensitive IT applications : The interaction of culture values and privacy issues in the Middle East. *Information Technology & People*, 16(1), 49-75.
<https://doi.org/10.1108/09593840310463023>
- Zang, Z., Zheng, Q., & Luo, L. (2022). Risk sensitivity mediates the relationship between construal level and ethical decision making. *Social Behavior and Personality: An International Journal*, 50(4), 1-11. <https://doi.org/10.2224/sbp.11309>
- Zhang, J., Beatty, S. E., & Walsh, G. (2008). Review and future directions of cross-cultural consumer services research. *Journal of Business Research*, 61(3), 211-224.
<https://doi.org/10.1016/j.jbusres.2007.06.003>
- Zhang, N.A., Wang, C., Karahanna, E., & Xu, Y. (2022). Peer Privacy Concern: conceptualization and measurement. *MIS Quarterly*, 46(1), 491-529.
- Zuboff, S. (2019). *The Age Of Surveillance Capitalism*. PublicAffairs.

Annexes

Annexe 1 : Exemple de notification de violations de données personnelles



Paris La Défense, le 19-nov-20

Objet : Information relative à la protection de vos données personnelles

Référence : YR-11875/E2C

Chère Madame, Cher Monsieur,

Vous recevez cette note d'information car avez souscrit, avant 2018, à titre personnel ou professionnel à un contrat de protection santé BNP Paribas géré par Mercer.



CI 0101
(B 12) - 5051 - 1/1 - 10101 - 5051 - A - 3011200779005

Mademoiselle AUBERT CHRISTELLE
8 AVENUE DE BONNELLES
78320 LE MESNIL ST DENIS

La protection et la sécurité de vos données personnelles sont de la plus haute importance pour Mercer. A ce titre, nous tenons à vous informer d'un incident de sécurité relatif à vos données personnelles intervenu chez l'un de nos prestataires informatiques, Visiativ. Cette note d'information a pour objet de vous préciser les détails de l'incident, les actions entreprises par les différentes parties et les modalités pratiques pour nous joindre en cas de questions.

En septembre 2020, Mercer a été informé par Visiativ que l'un de leurs salariés avait, sans autorisation, téléchargé un répertoire informatique comportant de multiples fichiers sur un serveur de stockage personnel dans le « cloud ». Le répertoire, ainsi téléchargé, s'est trouvé par la suite être aspiré par des tiers non autorisés. Parmi ces fichiers, l'un appartenait à Mercer. Ce fichier avait été partagé en 2018 avec Visiativ, de manière chiffrée, afin de remédier à un problème technique.

Vous recevez cette note d'information conformément à l'Article 34 du Règlement Général sur la Protection des Données (RGPD) car votre nom, prénom et numéro de Sécurité sociale figuraient dans ce fichier. Aucune autre donnée personnelle telle que votre adresse email, votre numéro de téléphone, vos informations financières ou de santé n'y étaient présentes. Cet incident n'a pas non plus eu de répercussions sur les opérations de Mercer ou sur votre couverture assurantielle et autres services qui vous sont fournis par Mercer.

Mercer a travaillé en étroite collaboration avec Visiativ pour gérer l'incident. Mercer a également notifié cette violation à l'autorité française de protection des données (la CNIL : Commission Nationale de l'Informatique et des Libertés).

Nous considérons que cet incident crée pour vous un risque limité compte tenu des modalités techniques de stockage de vos données personnelles dans ledit fichier. Néanmoins, Mercer et Visiativ ont mis en place une surveillance internet afin de détecter toute publication ou apparition des données impactées. A ce jour, la surveillance n'a pas détecté de diffusion publique de ces données.

Nous vous recommandons d'être vigilant notamment vis-à-vis de la réception de courriers électroniques ou de courriers postaux suspects ou de tout autre événement inhabituel impliquant vos données personnelles. Pour plus de précisions sur les moyens de protection de vos données personnelles, nous vous invitons à visiter le site www.cybermalveillance.gouv.fr/bonnes-pratiques.

Nous vous prions d'accepter nos sincères excuses pour les désagréments causés par cet incident. Nous reconnaissons l'importance de la protection de la vie privée et de la sécurité des données personnelles et continuons à travailler avec la plus grande détermination pour prévenir tout incident futur.

Si vous avez des questions ou si vous souhaitez de plus amples précisions, n'hésitez pas à contacter nos équipes dédiées par téléphone du lundi au vendredi de 9h à 17h au 0800 94 48 40 (numéro non surtaxé).

Bien cordialement,
Vincent Harel, Président Mercer France

Pour plus d'information sur notre politique de confidentialité Mercer, nous vous invitons à visiter la page dédiée à cet effet sur notre site web : www.mercer.fr/confidentialite.

Mercer (France) SAS, Société de Courtage en Assurances, dont le siège social est situé Tour Ariane, 5 Place de la Pyramide, 92800 Puteaux, immatriculée au RCS de Nanterre n° 390 589 455 dont le capital social est de 30 539 670 euros et enregistrée auprès de l'Organisme pour le Registre des Intermédiaires en Assurance (ORIA) n°07001885 (www.oria.fr). Service Réclamation Clients : Tour Ariane, 5, place de la Pyramide, 92800 Puteaux. Service de médiation : La Médiation de l'Assurance, TSA 50110, 75441 Paris Cedex 09. ACPRI, 4, place de Budapest, CS 92459, 75436 Paris Cedex 09.



Annexe 2 : Ensemble des recherches interculturelles en vie privée

#	Auteurs	Année	Titre	Journal
1	Altman	1977	Privacy Regulation: Culturally Universal or Culturally Specific?	Journal of Social Issues
2	Milberg et al.	1995	Values, personal information privacy, and regulatory approaches	Communications of the ACM
3	Maynard & Taylor	1996	A comparative analysis of Japanese and U.S. attitudes toward direct marketing	Journal of Direct Marketing
4	Milberg et al.	2000	Information Privacy: Corporate Management and National Regulation	Organization Science
5	Zakaria et al.	2003	Designing and implementing culturally-sensitive IT applications: The interaction of culture values and privacy issues in the Middle East	Information Technology & People
6	Bellman et al.	2004	International Differences in Information Privacy Concerns: A Global Survey of Consumers	The Information Society
7	Dinev et al.	2006	Privacy calculus model in e-commerce – a study of Italy and the United States	European Journal of Information Systems
8	Steenkamp & Geyskens	2006	How Country Characteristics Affect the Perceived Value of Web Sites	Journal of Marketing
9	Muk	2007	Cultural influences on adoption of SMS advertising: A study of American and Taiwanese consumers	Journal of Targeting, Measurement and Analysis for Marketing
10	Hann et al.	2007	Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach	Journal of Management Information Systems
11	Cho et al.	2009	A multinational study on online privacy: global concerns and local responses	New Media & Society
12	Gurău & Ranchhod	2009	Consumer privacy issues in mobile commerce: A comparative study of British, French and Romanian consumers	Journal of Consumer Marketing
13	Posey et al.	2010	Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities	European Journal of Information Systems
14	Krasnova & Veltri	2010	Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA.	43rd Hawaii International Conference on System Sciences
15	Lowry et al.	2011	Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The	Journal of Management

			Case of Instant Messaging in Two Cultures	Information Systems
16	Tsoi & Chen	2011	From Privacy Concern to Uses of Social Network Sites: A Cultural Comparison via User Survey. Privacy, Security, Risk and Trust	Third International Conference on Social Computing
17	Krasnova et al.	2012	Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus	Business & Information Systems Engineering
18	Chen et al.	2013	A Cross-Culture Empirical Study of M-commerce Privacy Concerns	Journal of Internet Commerce
19	Miltgen & Peyrat-Guillard	2014	Cultural and generational influences on privacy concerns: a qualitative study in seven European countries	European Journal of Information Systems
20	Cecere, Le Guel & Soulié	2015	Perceived Internet privacy concerns on social network in Europe	Technological Forecasting and Social Change
21	Park et al.	2015	Consumer characteristics and the use of social networking sites: A comparison between Korea and the US	International Marketing Review
22	Yang & Kang	2015	Exploring Big Data and Privacy in Strategic Communication Campaigns: A Cross-Cultural Study of Mobile Social Media Users' Daily Experiences	International Journal of Strategic Communication
23	Pentina	2016	Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison	Computers in Human Behavior
24	James et al.	2017	Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use	Information & Management
25	Trepte et al.	2017	A Cross-Cultural Perspective on the Privacy Calculus	Social Media + Society
26	Li et al.	2017	Cross-Cultural Privacy Prediction	Proceedings on Privacy Enhancing Technologies
27	Liu & Wang	2018	How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison	Information & Management
28	Li et al.	2022	Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites	Behaviour & Information Technology

Annexe 3 : Ensemble des Data Protection Authorities (DPA) en Europe

Les DPA sont les autorités administratives nationales pour la protection des données personnelles en Europe

Pays	Autorité	Site web
Autorité européenne	European Data Protection Board	https://edpb.europa.eu/about-edpb/board/members_fr
Allemagne	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	http://www.bfdi.bund.de/
Autriche	Österreichische Datenschutzbehörde	http://www.dsb.gv.at/
Belgique	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)	https://www.autoriteprotectiondonnees.be/ https://www.gegevensbeschermingsautoriteit.be/
Bulgarie	Commission for Personal Data Protection	https://www.cpdp.bg/
Chypre	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/
Croatie	Croatian Personal Data Protection Agency	http://www.azop.hr/
Danemark	Datatilsynet	http://www.datatilsynet.dk/
Espagne	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/
Estonie	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	http://www.aki.ee/
Finlande	Office of the Data Protection Ombudsman	http://www.tietosuoja.fi/en/
France	Commission Nationale Informatique et Libertés - CNIL	http://www.cnil.fr/
Grèce	Hellenic Data Protection Authority	http://www.dpa.gr/
Hongrie	Hungarian National Authority for Data Protection and Freedom of Information	http://www.naih.hu/
Italie	Garante per la protezione dei dati personali	http://www.garanteprivacy.it/
Irlande	Data Protection Commission	http://www.dataprotection.ie/
Lettonie	Data State Inspectorate	http://www.dvi.gov.lv/
Lituanie	State Data Protection Inspectorate	https://vdai.lrv.lt/
Luxembourg	Commission Nationale pour la Protection des Données	http://www.cnpd.lu/
Malte	Office of the Information and Data Protection Commissioner	http://www.idpc.org.mt/

Pays Bas	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl
Pologne	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/
Portugal	Comissão Nacional de Proteção de Dados - CNPD	http://www.cnpd.pt/
République tchèque	Office for Personal Data Protection	http://www.uoou.cz/
Roumanie	The National Supervisory Authority for Personal Data Processing	http://www.dataprotection.ro/
Slovaquie	Office for Personal Data Protection of the Slovak Republic	http://www.dataprotection.gov.sk/
Slovénie	Information Commissioner of the Republic of Slovenia	https://www.ip-rs.si/
Suède	Swedish Authority for Privacy Protection	https://www.imy.se/
Islande *	Persónuvernd	https://www.personuvernd.is or https://www.dpa.is
Liechtenstein *	Data Protection Authority, Principality of Liechtenstein	https://www.datenschutzstelle.li
Norvège *	Datatilsynet	www.datatilsynet.no

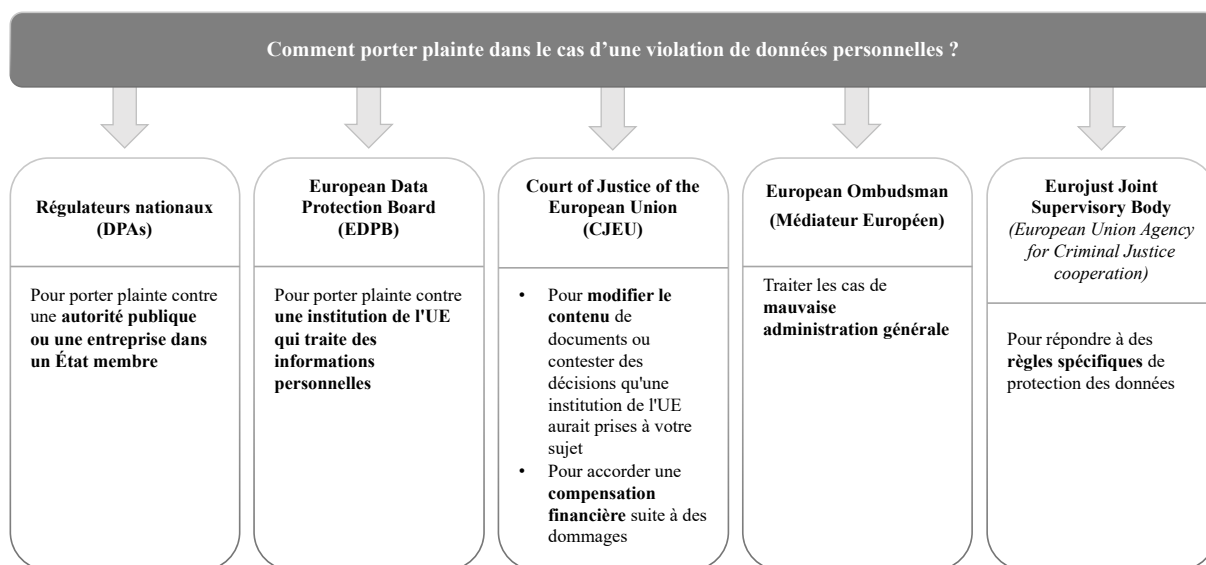
* Conformément à l'accord sur l'Espace économique européen (EEE), à compter du 20 juillet 2018, les pays de l'EEE, l'Islande, le Lichtenstein et la Norvège, sont devenus membres du conseil d'administration sans droit de vote et sans droit d'être élu en tant que président et vice-président, pour les questions liées au RGPD.

Annexe 4 : Principales théories mobilisées dans les recherches en vie privée (Li, 2012)

Catégorie	Théorie	Explications
Expliquent les antécédents à la préoccupation pour la vie privée	Agency theory	L'agent (e.g., site Web) peut se comporter de manière opportuniste pour maximiser ses intérêts, et génère alors des coûts supplémentaires pour le principal (e.g., le client). Divers mécanismes peuvent être utilisés pour aligner les intérêts de l'agent sur ceux du principal.
	Social contract theory (Donaldson & Dunfee, 1994)	Les utilisateurs, la communauté et l'industrie se comportent de manière équitable si leurs pratiques commerciales sont régies par un contrat social, (i) initié lorsque des normes sociales (i.e., obligations généralement comprises) régissent le comportement des personnes impliquées, et (ii) les contrats sociaux sont basés sur un consentement éclairé soutenu par un droit de sortie.
Mettent en lumière les compromis en matière de vie privée	Privacy calculus theory	L'intention d'un individu de divulguer des informations se fonde sur un calcul coût-bénéfice, entre les risques et les bénéfices attendus.
	Utility maximisation theory	Le comportement du consommateur est guidé vers la maximisation de l'utilité d'une action (i.e., le calcul de l'utilité de la protection de la vie privée) ou de la satisfaction totale reçue de la consommation d'un bien ou d'un service.
	Expectancy theory of motivation (Vroom, 1964)	La motivation d'un comportement est déterminée par l'opportunité du résultat. Le processus cognitif permettant de déterminer la pertinence et la motivation d'un comportement se déroulerait en 3 étapes : (i) l'attente qu'un certain effort conduise à la performance attendue, (ii) l'instrumentalité de cette performance pour atteindre un certain résultat, (iii) l'opportunité (appelée valence) de ce résultat pour l'individu.
	Expectancy value theory	Pour expliquer l'attitude d'une personne envers un objet / une action, cette théorie suggère que l'attitude naît inévitablement lorsqu'une personne forme des croyances sur l'objet / l'action. Même si des différences sur un objet / une action sont formées, seules les croyances facilement accessibles dans la mémoire (ex. les risques associés à une action) influencent l'attitude à un moment donné
Expliquent les conséquences comportementales	Theory of reasoned action (TRA) (Ajzen & Fishbein, 1975)	Dans le prolongement de l'expectancy-value theory, la TRA indique que l'attitude d'une personne à l'égard du comportement et la norme subjective déterminent l'intention comportementale, qui elle-même détermine le comportement volontaire d'une personne.
	Theory of planned behaviour (TPB)	Dans la continuité de la TRA, la TPB indique que le contrôle comportemental d'une personne, en plus de l'attitude et de la norme subjective, influence l'intention comportementale.
Identifient les facteurs influenceurs institutionnels	Procedural fairness theory (ou justice theory)	L'équité procédurale contribue à instaurer la confiance lorsque les agents (sites web) exercent un pouvoir délégué important au nom des clients. Pour apaiser les inquiétudes des clients et rendre justice, les processus de décision des agents doivent être transparents pour les clients.

	Social presence theory	Dans le contexte de la communication assistée par ordinateur, classe les moyens de communication le long d'un continuum unidimensionnel de présence sociale, définie comme le niveau de conscience de l'interlocuteur pendant une interaction de communication.
	Social response theory	Une personne s'engage dans la divulgation d'informations personnelles si elle est le destinataire d'une divulgation similaire de la part d'une autre personne, d'une organisation et même d'un ordinateur. Ce faisant, une norme de réciprocité se développe entre les deux, ce qui encourage davantage la divulgation d'informations intimes.
Identifient les facteurs influenceurs individuels	Protection motivation theory	Développée pour expliquer les effets de frayeur et de peur sur les attitudes et les comportements, cette théorie suggère que l'intention d'un individu de se protéger des menaces potentielles dépend de quatre facteurs : (1) la gravité perçue d'un événement menaçant, (2) la probabilité perçue que l'événement se produise, (3) l'efficacité du comportement préventif recommandé qu'un individu s'attend à adopter, et (4) la capacité perçue de l'individu à adopter le comportement préventif recommandé.
	Information boundary theory	Processus cognitif consistant à gérer les limites des espaces de communication, en trouvant un équilibre entre le besoin de divulgation et le besoin de confidentialité. Ces limites peuvent être lâches ou contrôlées en fonction du degré de risque associé à la confidentialité de l'information.
	Social cognitive theory	Dans la continuité des 2 théories précédentes (qui soulignent l'importance des capacités individuelles à gérer les risques liés à la vie privée), et développée à partir de la théorie de l'apprentissage social, cette théorie postule que l'acquisition de connaissances d'un individu peut être directement liée à l'observation des autres dans le contexte des interactions et expériences sociales (les gens apprennent en observant et en expérimentant). Ainsi, un élément clé de l'apprentissage en tant que processus cognitif est l'auto-efficacité, i.e., la croyance d'une personne en sa propre compétence à accomplir une tâche.
	Personality theory	Cette théorie suggère que divers traits de personnalité, (i.e., ouverture, conscience, extraversion, agréabilité et stabilité émotionnelle ; cf. Big Five), influencent les processus cognitifs, les attitudes et les comportements vis-à-vis de la vie privée.

Annexe 5 : Autorités européennes compétentes dans le traitement de plaintes pour violations de données personnelles



Annexe 6 : Modalités de dépôt de plainte sur le site Internet du DPA irlandais

The sequence of screenshots illustrates the process of filing a complaint on the Irish Data Protection Commission (DPC) website:

- Homepage:** The user is on the DPC homepage. A red arrow points from the 'Take Action' section (specifically 'REPORT A BREACH', 'RAISE A CONCERN', or 'REGISTER YOUR DPO') to the 'Contact Us' link in the top navigation bar.
- Contact Us Page:** The user is on the 'Contact Us' page. A red arrow points from the 'Contact Us Online' link to the 'Preliminary Questions' section.
- Preliminary Questions Form:** The user is answering preliminary questions. A red arrow points from the 'Preliminary Questions' section to the 'Contact the Data Protection Commission with a general query' form.
- Contact Form:** The user is on the 'Contact the Data Protection Commission with a general query' form, which includes fields for 'Full Name', 'Your Phone number', 'Your Email Address', and a text area for 'Please enter the reason you are contacting Data Protection Commission:'.

Annexe 7 : Scores des dimensions d'Hofstede pour les pays européens

Source : <https://www.hofstede-insights.com/fi/product/compare-countries/>

Les pays sont classés par ordre décroissant selon le score d'Individualisme.

Pays	Power distance	Individualism	Masculinity	Uncertainty_avoidance	Long term orientation	Indulgence
Royaume-Uni	35	89	66	35	51	69
Hongrie	46	80	88	82	58	31
Pays Bas	38	80	14	53	67	68
Italie	50	76	70	75	61	30
Belgique	65	75	54	94	82	57
Danemark	18	74	16	23	35	70
France	68	71	43	86	63	48
Suède	31	71	5	29	53	78
Lettonie	44	70	9	63	69	13
Irlande	28	70	68	35	24	65
Allemagne	35	67	66	65	83	40
Finlande	33	63	26	59	38	57
Luxembourg	40	60	50	70	64	56
Pologne	68	60	64	93	38	29
Estonie	40	60	30	60	82	16
Lituanie	42	60	19	65	82	16
Malte	56	59	47	96	47	66
République tchèque	57	58	57	74	70	29
Autriche	11	55	79	70	60	63
Slovaquie	100	52	100	51	77	28
Espagne	57	51	42	86	48	44
Grèce	60	35	57	100	45	50
Croatie	73	33	40	80	58	33
Roumanie	90	30	42	90	52	20
Bulgarie	70	30	40	85	69	16
Slovénie	71	27	19	88	49	48
Portugal	63	27	31	99	28	33

Annexe 8 : Formulaire de pré-entretien de l'essai 2 niveau Méso

Formulaire

Nom

Prénom

Nom de famille

Quel est votre lieu de résidence ?

Avez-vous ?

- ☐ moins de 19 ans
☐ entre 19 et 24 ans
☐ entre 25 et 44 ans
☐ entre 45 et 64 ans
☐ plus de 65 ans

Quelle activité exercez-vous actuellement ?

Avez-vous exercé d'autres activités auparavant différentes de celle-ci ? Si oui, lesquelles ?

Diriez-vous que vous utilisez des moyens et des outils informatiques vous permettant de protéger votre vie privée en ligne ?

- ☐ Oui
☐ Non
☐ Je ne sais pas

Diriez-vous que vous êtes actif au sein d'associations, dans le milieu militant ou sur les réseaux sociaux, en matière de protection des données personnelles et de la vie privée en ligne ?

- ☐ Oui, très actif
☐ Plutôt moyennement actif
☐ Non, pas du tout actif
☐ Je ne sais pas

Avez-vous déjà porté plainte à la CNIL (Commission Nationale Informatique et Libertés en France) ?

- ☐ Oui
☐ Non

Avez-vous déjà lancé une action de plainte ou une action en justice pour risque ou vol avéré de données personnelles ?

- ☐ Oui
☐ Non
☐ Je ne sais pas
☐ Saisissez l'option 4

Je vous remercie sincèrement d'avoir pris le temps de répondre à ces questions.

Nous nous parlons donc très vite par visio.

Excellente journée à vous,

Christelle

—

Christelle Aubert Hassouni

Doctorante ESCP Business School & Privacy Researcher

christelle.aubert Hassouni@protonmail.com

Soumission

Annexe 9 : Guide d'entretien de l'essai 2 niveau Méso

- *Consignes d'usage et remerciements d'avoir répondu au questionnaire préalable*

1. Valider les comportements de protection de la vie privée et des données personnelles

- *Vous avez indiqué utiliser plusieurs moyens pour protéger votre vie privée*
- *Pouvez-vous me décrire ces actions ?*
- *Vous n'avez jamais mené d'actions en justice : pourquoi ?*
- *Ces actions sont-elles plus efficaces : en groupe, individuelles ou au niveau national ?*

2. Vérifier l'appartenance à un groupe social

- *Je vous ai contacté suite à votre tweet faisant état de votre plainte à la CNIL (modifié selon les personnes interrogées). Vous m'avez confirmé être très engagé en associatif et militant pour la protection de la vie privée.*
- *Est-ce vrai ? Depuis combien de temps faites-vous cela ?*
- *Pourquoi faites-vous cela ? Quel est l'objectif de ces différentes actions ?*
- *Quel est votre rôle au sein de ces associations et quelles sont vos relations avec les membres ?*

3. Identifier les valeurs et le chaînage cognitif des actions de groupe (Moyens – Fins)

- *Je vous propose de reprendre chacune des actions (associations, actions techniques ...) et de parler à chaque fois du **comment** et du **pourquoi** de ces actions.*
 - *Quels sont les avantages, en termes de moyens, de ces actions ?*
 - *Relancez si nécessaire : Est-elle facile, efficace, complexe, peu chère etc. ?*
 - *Quels sont les avantages, en termes d'objectifs, de ces actions ?*
 - *A quoi sert cette action ? quels sont ses objectifs ? que cherchez-vous à atteindre ?*
 - *Pourquoi cela est-il important pour vous ?*
 - *Relancez pas à pas pour faire le lien attribut – caractéristiques*
- *Si vous deviez décrire la personne active pour la protection de la vie privée en ligne, comment le feriez-vous ? Quelles seraient ses valeurs, les aspects moraux importants pour elle ?*
 - *Relancez si nécessaire : indépendance, liberté, responsabilité, ... ?*
 - *Vous êtes engagé : diriez-vous que vous êtes quelqu'un dont les valeurs importantes sont ... (citer les valeurs citées à la question précédente) ?*

4. Identifier les réactions face à une violation de données personnelles :

- *Si vous apprenez ce matin que la Caisse d'Assurance Maladie a fait l'objet cette nuit d'un gros hacking et que vos données sont dévoilées. Que faites-vous ? pourquoi ?*

Remerciements

Annexe 10 : Principaux résultats d'une recherche sur les motifs de recours au droit menée par la CNIL

La CNIL a publié en avril 2021 un cahier IP8¹⁴⁵, pour explorer le rapport quotidien à la protection des données personnelles et les situations problématiques du recours au droit. Cette analyse fait ressortir 4 situations de recours au droit (protection de réputation en ligne, intrusion de la prospection commerciale, surveillance au travail, inscription jugée induite dans des fichiers nationaux) et 3 conditions du dépôt de plainte à la CNIL (représentation concrète de l'infrastructure de données, sentiment de victimisation, incapacité à régler la situation seul).

Suite à cela, et afin d'approfondir la compréhension des motivations de dépôt de plainte à la CNIL, celle-ci a réalisé une enquête auprès de plaignants, par questionnaire (N=284), et en face à face (N=105). Nous avons échangé le 25.02.2022 avec Antoine Courmont, chargé d'études prospectives à la CNIL, qui a partagé les principaux résultats de cette enquête :

1. Les principaux motifs de plainte sont la prospection commerciale et la surveillance au travail. Ces motifs restent relativement constants dans le temps et étaient déjà présents dans les années 80.
2. Les plaignants sont des hommes (62%), diplômés (Master +), CSP+, résidant en Ile de France.
3. Les plaintes sont essentiellement des plaintes individuelles. Il y a très peu de plaintes collectives, et dans ce cas, ce sont surtout gens très techniques et très au fait de la loi.
4. Le dépôt de plainte vise surtout à résoudre un problème individuel, pour les raisons suivantes : (i) finalité militante (mais minorité), (ii) par attachement au respect du droit, (iii) par culture du risque (sensibilisés au sujet, souvent ayant une bonne culture IT), (iv) car affecte la vie quotidienne (e.g., refus de prêt, victime de harcèlement), (v) car somme de désagrément (« spam de trop »), (vi) par logique de signalement, (v) car mauvaise relation avec l'organisme (surtout s'il s'agit d'une grande entreprise).
5. Le cadre professionnel joue un rôle majeur dans la sensibilisation à la protection de la vie privée. Par contre, c'est un sujet très peu abordé avec des proches car il s'agit d'un comportement marginal et souvent moqué, hormis pour les activistes.

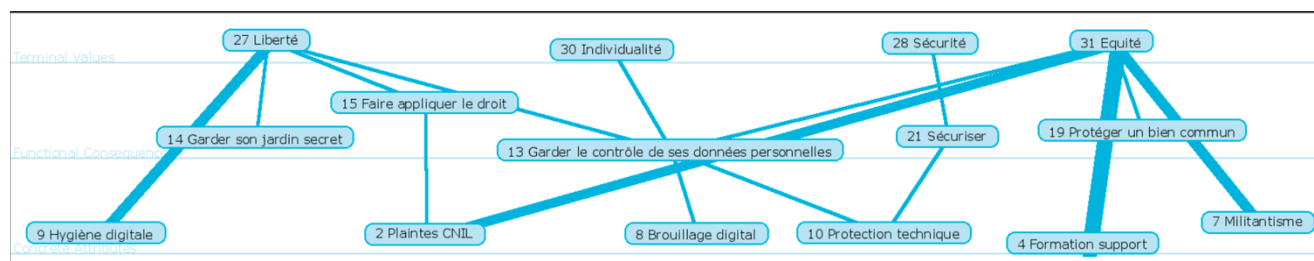
¹⁴⁵ IP8 « Scènes de la vie numérique » disponible à : <https://linc.cnil.fr/fr/cahier-ip8-scenes-de-la-vie-numerique-une-exploration-du-rapport-quotidien-la-protection-des-donnees>

6. Exercer ses droits et porter plainte reste très complexe et demande beaucoup de temps. Par conséquent, certains deviennent des professionnels du dépôt de plainte et 27% des plaignants ont déposé plus d'une plainte.
7. Les associations de consommateurs sont très minoritaires
8. Les pratiques déclarées sont très variables et la pratique qui ressort le plus est l'usage de multiples adresses e-mail.

Annexe 11 : Matrice d'implication de l'essai 2 niveau Méso

IMPLICATION MATRIX	Liberté	Sécurité	Transparence	Individualité	Equité
Signalement	0 2				0 3
Plaintes CNIL	0 3		0 3		0 5
Recours en justice		0 1			0 1
Formation support	0 2				0 9
Sensibilisation	0 3	0 1		0 2	0 3
Name showing			0 3		0 1
Militantisme	0 1			0 1	0 5
Brouillage digital	0 6	0 2		0 5	0 3
Hygiène digitale	0 5	0 1		0 4	0 1
Protection technique	0 4	0 5	0 1	0 5	0 4
Limiter le SPAM				3 0	
Limiter le scoring	1 0			2 0	
Garder le contrôle de ses données personnelles	7 0	1 0	1 0	9 0	6 0
Garder son jardin secret	5 0				
Faire appliquer le droit	5 0	1 0	1 0		2 0
Sensibiliser au risque	1 0	1 0		1 0	
Former à la technologie	1 0				2 0
Développer des actions de groupe	1 0				2 0
Protéger un bien commun	1 0		1 0		10 0
Rendre la technologie positive					3 0
Sécuriser	3 0	6 0			
Permettre l'anonymat	1 0	1 0			3 0
Dénoncer les entreprises non respectueuses			4 0		2 0
Freiner l'économie des données				1 0	
Limiter la surveillance étatique				1 0	1 0
Militer pour des idéologies					4 0
Liberté					
Sécurité					
Transparence					
Individualité					
Equité					
sum	26 26	10 10	7 7	17 17	35 35

Annexe 12 : Carte hiérarchique de l'essai 2 niveau Méso



cut-off values = 5

Annexe 13 : Structure du questionnaire de l'essai 3 niveau Micro

Introduction et question piège		
Partie 1 : questions sur les préférences culturelles	40 items présentés de manière aléatoire	Échelle de Likert à 7 niveaux (de « pas du tout d'accord » à « tout à fait d'accord »)
Partie 2 : scénarios de violations de données (présentation d'une situation et questions sur les réponses apportées à cette situation, les réponses pouvant aller de « ne rien faire » au « recours en justice »)	Scenario 0 : comportement dans le cas d'un achat insatisfait Scenario 1 : réponses apportées face à une fuite de données d'un site marchand ou d'un réseau social fréquenté régulièrement Scenario 2 : réponses apportées à un débit d'argent inattendu sur un compte bancaire	Échelle de Likert à 7 niveaux (de « absolument pas probable » à « très fortement probable »)
Partie 3 : mesure de la distance psychologique	10 items présentés de manière aléatoire : 3 items pour la distance sociale 3 items pour la distance géographique 3 items pour la distance hypothétique 1 item avec curseur de réponse pour la distance temporelle	Échelle de Likert à 7 niveaux (de « pas du tout d'accord » à « tout à fait d'accord »)
Partie 4 : mesure de la privacy self-efficacy et des normes subjectives	3 items pour les normes subjectives 2 items pour la <i>privacy self-efficacy</i>	Échelle de Likert à 7 niveaux (de « pas du tout d'accord » à « tout à fait d'accord »)
Partie 5 : mesure de la <i>privacy concern</i>	4 items présentés de manière aléatoire	Échelle de Likert à 7 niveaux (de « cela ne me préoccupe pas du tout » à « cela me préoccupe énormément »)
Partie 6 : mesure d'une précédente violation de données personnelles	Présentation de 8 cas de violations de données (e.g., piratage du réseau de l'entreprise, prise en main de son téléphone) et interrogation sur le vécu de cette situation	3 réponses possibles : « Jamais », « il y a moins d'un an », « il y a plus d'un an »
Partie 7 : questions sociodémographiques		

Annexe 14 : Caractéristiques de l'échantillon interrogé dans l'essai 3 niveau Micro

		%	N
Sexe	Homme	53,3%	
	Femme	46,7%	
	Total	100%	452
Age	18-24 ans	5.5%	25
	25-44 ans	46.5%	211
	45-64 ans	39.4%	178
	Plus de 65 ans	8.5%	38
	Total	100%	452
	Moyenne	44.84 ans	
Professions	Employés	28.1%	127
	Professions intermédiaires	16.2%	73
	Retraités	14.8%	67
	Cadres et professions intellectuelles supérieures,	14.2%	64
	Ouvriers	8.2%	37
	Demandeurs d'emploi	6.0%	27
	Au foyer ou sans emploi	5.8%	26
	Autres	6.7%	31
	Total	100%	452

Influence de la culture sur les réponses face à une violation de données personnelles

Les recherches portant sur l'influence de la culture sur la préoccupation pour la protection de la vie privée explorent principalement le lien entre préférence culturelle à l'individualisme (i.e., défense de ses propres objectifs) et souci de protection de ses données personnelles. Or elles font face à des contradictions. De plus, les comportements face à des violations de données personnelles restent encore peu compris. En faisant varier les angles d'observation, cette recherche tente d'apporter un éclairage nouveau. Nous montrons qu'une préférence culturelle pour des valeurs d'égalité sociale et de genre amène les individus à adopter des réponses (techniques, sociales ou institutionnelles) plus actives face à une violation de leurs données. Cette préférence opère à trois niveaux : (1) macro, les individus vivant dans des pays valorisant l'égalité des genres ayant davantage tendance à se plaindre, (2) méso, la protection de la vie privée étant envisagée comme une pratique sociale mobilisant des techniques, des compétences et des idéaux comme la défense de l'égalité sociale, (3) micro, l'égalité sociale et de genre étant une valeur culturelle impliquant moins de distance psychologique avec la violation de données. Cette mise en lumière apporte une compréhension théorique novatrice de la préoccupation pour la protection de la vie privée, envisagée comme un « mieux vivre ensemble » et comme un souci de sécuriser les données personnelles de tous. Notre recherche permet aussi d'enrichir la compréhension des réponses aux violations de données personnelles et de leurs mécanismes. Ainsi, des possibilités d'actions sont proposées aux politiques publiques et aux acteurs de la cybersécurité.

Violations de données personnelles ; réponses pour la protection de la vie privée ; valeurs culturelles.

Influence of culture on responses to a personal data breach

Research on the influence of culture on privacy concerns has largely focused on links between cultural preference for individualism (i.e., advocacy for one's own goals) and concern for personal data protection. However, these studies are contradictory. Moreover, the current understanding of behaviors associated with breaches of personal data is quite poor. This study attempts to shed new light on this topic through a new observational approach. We show that a cultural propensity for values of social and gender equality pushes individuals to adopt more active responses (technical, social or institutional) to breaches of their personal data. This propensity operates at three levels: (1) macro, individuals living in countries valuing gender equality leading them to complain more, (2) meso, with privacy protection envisaged not as an individual practice, but rather a social one that mobilizes techniques, skills, but also ideals, acting mainly as a defense of social equality, (3) micro, with cultural values of social and gender equality implying less psychological distance with data breaches. This insight provides a novel theoretical understanding of the concern for personal privacy as a 'better life together' and not a 'better life alone' as well as a concern for securing everyone's personal data. Our research also builds theoretical understanding of responses to personal data breaches and their mechanisms. Possible courses of action are thus proposed to public policies and cybersecurity actors.

Personal data breaches; privacy responses; cultural values.