Université de Montréal

La vie privée à l'ère des données massives

Par

Rose Landry

Département de philosophie Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître ès arts (M.A.) en Philosophie, option recherche avec mémoire long

Février 2022

Université de Montréal

Département de philosophie Faculté des arts et des sciences

Ce mémoire intitulé

La vie privée à l'ère des données massives

Présenté par

Rose Landry

Évalué par un jury composé des personnes suivantes

Christine Tappolet

Président-rapporteur

Christian Nadeau

Directeur de recherche

Marc-Antoine Dilhac

Membre du jury

Résumé

Ce mémoire propose une analyse conceptuelle de la vie privée et des enjeux éthiques qui s'y rapportent à l'ère des données massives et de l'essor de l'intelligence artificielle. Alors que la définition du concept de vie privée est encore disputée, les défis liés à son maintien dans le monde numérique d'aujourd'hui sont indéniables. L'analyse de ces enjeux requiert de faire appel à des éléments conceptuels provenant de la philosophie de l'information, mais également aux notions de structures de pouvoir tirées de la philosophie politique et de la sociologie. À travers ce prisme, ce travail offre un survol des éléments essentiels au traitement des enjeux de vie privée dans le contexte actuel d'utilisation des données massives, et défend qu'en l'absence de processus adéquats pour protéger et préserver la vie privée d'une personne en ligne, la capacité à maintenir une vie privée numérique devient illusoire. En définitive, un argument moral en faveur d'une meilleure protection de la vie privée en ligne est présenté, démontrant que la vie privée est notamment garante de l'autonomie des personnes.

Mots clés : vie privée ; données massives ; éthique appliquée ; philosophie de l'information ; intelligence artificielle.

Abstract

This essay provides a conceptual analysis of privacy and the ethical issues that surround it in the age of big data and artificial intelligence. While the definition of privacy is still disputed, the challenges of maintaining it in today's digital world are undeniable. In order to analyze these challenges, one can combine conceptual elements taken from the philosophy of information with notions of power found in political philosophy and sociology. Through this lens, this paper offers an overview of how one can address privacy-related ethical concerns in the current context of massive data collection, analysis and use. It is argued that, without adequate processes in place to protect and preserve one's privacy online, the ability to maintain digital privacy becomes illusory. This paper concludes by providing a moral argument to demonstrate how privacy can be better preserved online, demonstrating that privacy is notably a condition of personal autonomy.

Keywords : privacy ; big data ; applied ethics ; information philosophy ; artificial intelligence.

Table des matières

LISTE DES SIGNES & ABRÉVIATIONS

GAFAM	Acronyme référant aux géants technologiques Google, Apple, Facebook, Amazon et Microsoft.
IA	Intelligence artificielle
RGPD	Règlement Général sur la Protection des Données

REMERCIEMENTS

Je tiens à exprimer ma gratitude à toutes les personnes qui ont su, de près ou de loin, m'encourager et me guider tout au long de la rédaction de ce mémoire. Le soutien que j'ai reçu au cours de mes études a pris de multiples formes et je suis reconnaissante pour chacune d'elles.

À Robert et Nadia, pour m'avoir toujours poussé à dépasser mes limites et pour m'avoir enseigné à mener à terme mes projets.

À Louis, mon ancre, d'avoir partagé avec moi mes hauts et mes bas, mes joies et mes peines tout au long de cette épreuve.

À mes amies, ces femmes d'une force et d'une intelligence remarquables, que j'admire profondément et qui m'inspirent au quotidien.

À Gabrielle pour ses relectures et commentaires qui ont non seulement contribué à améliorer grandement la qualité de ce mémoire, mais qui m'ont également redonné confiance dans les moments où mon projet m'apparaissait complètement farfelu.

À Judith, qui sans le savoir m'a donné l'élan d'énergie nécessaire pour continuer d'avancer alors que je désirais tout arrêter.

Enfin, milles mercis à Christian Nadeau pour son soutien constant, et ce malgré mes longs silences. Je le remercie pour son approche humaine, ses encouragements et ses nombreuses relances!

INTRODUCTION

Dans un monde où les nouvelles technologies de l'information prennent une place croissante, leurs impacts sur les modes de vie font naître de nombreuses tensions dans les sociétés dont les valeurs se retrouvent en conflit. D'un côté, se fait sentir une tendance au positivisme technologique, soit une propension à embrasser ces nouvelles technologies indépendamment de leurs effets négatifs potentiels. Ceci s'explique notamment par le fort attrait de ces technologies, qui offrent des possibilités inégalées de progrès dans de nombreux domaines pouvant impacter de façon positive les sociétés. De l'autre côté, elles posent de nombreux enjeux en matière d'équité, de justice et de droits de la personne. Ces nouvelles technologies exercent en effet de nombreuses pressions sur les systèmes de valeurs des sociétés offrant à la fois des avantages non négligeables, mais ouvrant en même temps la porte à une série de conséquences négatives. On assiste ainsi à une montée en tension entre des valeurs et intérêts en opposition. Depuis les révélations d'Edward Snowden[1], et plus récemment l'affaire Cambridge Analytica[2], la question de la protection de la vie privée est devenue un enjeu central parmi ceux suscités par les récentes innovations dans les technologies de l'information. En effet, ces dernières reposent largement sur l'utilisation de données et la pression exercée sur l'accès aux données personnelles pose des enjeux sans précédent pour la protection de la vie privée. Ces enjeux sont d'autant plus complexes en raison de l'absence de consensus sur la signification et la valeur de la vie privée.

Les personnes tiennent généralement à leur vie privée et à la protection de leur intimité. Elles souhaitent avoir un certain contrôle sur qui sait quoi à leur sujet et ne veulent certainement pas que leurs informations personnelles soient accessibles à tout le monde en tout temps. En même temps, la signification et la valeur de la vie privée font l'objet de controverses, dans un monde où l'exposition de soi et le partage d'information sont rendus non seulement banals, mais glorifiés. La combinaison de la performance croissante des nouvelles technologies et du trouble entourant

[1]Antonio Casilli, « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », Etude annuelle 2014 du Conseil d'Etat, Le numérique et les droits fondamentaux (La Documentation Française, 2014), http://cvpip.wp.mines-telecom.

[2] Ikhlaq ur Rehman, « Facebook-Cambridge Analytica data harvesting: What you need to know », *Library Philosophy and Practice (e-journal)*, 2019.

la valeur accordée à la vie privée donne ainsi lieu à des enjeux de sociétés qui requièrent l'apport des philosophes. Comment concilier le progrès technologique et les valeurs sociales comme celle de protection de la vie privée? Et quelles sont la place et la valeur de cette dernière dans le monde connecté d'aujourd'hui? La vie privée serait-elle devenue une valeur désuète ou bien au contraire plus essentielle que jamais?

Ces questions demandent une attention particulière de la part des philosophes et éthiciens. Le présent mémoire n'a pas l'ambition de répondre à l'ensemble de ces questions. L'ampleur du travail nécessaire pour y apporter des réponses nécessitera l'apport de nombre d'académiciens, ainsi qu'une collaboration interdisciplinaire, entre les éthiciens, juristes, sociologues, politologues et les scientifiques qui développent les technologies dont nous traitons ici. Les enjeux en question sont trop complexes et leurs dimensions trop transversales pour qu'une seule discipline – encore moins une seule thèse – ne parviennent à les décortiquer convenablement.

Le présent mémoire propose une contribution au travail nécessaire de mise en place de bases théoriques. Plusieurs auteurs de la philosophie de l'information ont déjà entamé ce labeur, mais le champ d'études demeure encore jeune et les travaux philosophiques étudiant les relations entre le concept de vie privée et l'utilisation des données massives sont encore rares. Ainsi plutôt que de se pencher sur une question spécifique, nous proposons dans ce mémoire une définition du concept de vie privée et une présentation des enjeux particuliers liés à l'utilisation des données qui pourront ensuite servir pour de futurs travaux sur la question éthique de la protection de la vie privée dans le contexte numérique. Afin de démontrer la portée des bases théoriques présentées dans ce mémoire, nous proposons également un argument normatif démontrant la valeur de la vie privée numérique.

L'objectif de ce mémoire n'est pas de défendre la vie privée à tout prix ou d'en faire une valeur absolue, mais bien de rendre compte de la complexité des éléments qui contribuent actuellement à mettre en péril toute optique de vie privée numérique. Ce faisant, nous entendons contribuer au débat public sur la protection de la vie privée et fournir des arguments moraux en ce sens. Ce projet s'inscrit ainsi à l'intersection de plusieurs disciplines. Il est avant tout philosophique vu le travail d'analyse conceptuel qui y est accompli et conformément à son objectif visant à définir la vie privée et mieux saisir ses ambiguïtés. Les questions qui animent ce mémoire sont néanmoins ancrées dans des réflexions pratiques et concrètes, propres au monde

contemporain. Il est donc question d'un travail d'éthique appliquée. Enfin, il s'agit également d'un projet normatif, puisque nous y prenons position. Ce mémoire a donc non seulement une vocation académique de contribution au savoir, mais également politique, soit de contribuer à un débat de société pour peut-être l'influencer. Cet ancrage dans la réalité nous amènera d'ailleurs parfois à dépasser le champ philosophique pour intégrer des considérations juridiques, politiques et sociologiques, tant de domaines qui enrichissent la réflexion et participent à une meilleure compréhension des enjeux complexes qui seront traités.

Dans la première section de ce mémoire, nous nous attarderons au concept de vie privée, ses origines et ses propriétés. La définition de ce qu'est la vie privée ne faisant pas consensus, il nous faudra porter une attention particulière aux différents débats qui animent la littérature traitant de ce concept afin de bien situer ce dont il sera question pour la suite du mémoire. Après un bref retour sur l'histoire et les origines du concept, nous aborderons donc les trois principaux débats qui façonnent les différentes versions de la vie privée. Nous débuterons par l'enjeu existentiel, à savoir s'il existe effectivement une chose telle et singulière que la vie privée, ou bien s'il s'agit d'une construction sans utilité propre. Ensuite, nous examinerons la question de la charge normative du concept de vie privée, favorisant une définition descriptive du concept. Puis, nous terminerons avec la question de la nature de la vie privée, ou son « unité de référence ». Ces trois éléments d'analyse nous permettront de conclure sur une définition pour le concept de vie privée qui sera utilisé dans la suite du mémoire.

Au deuxième chapitre sont introduits les grands enjeux liés aux technologies de l'information, explorant la relation entre ces dernières et le concept de vie privée. Nous illustrerons les menaces spécifiques que posent les technologies de l'information, et plus spécifiquement que l'utilisation massive des données font peser sur la vie privée. La première section du chapitre se concentrera sur les données numériques, leur utilisation et les menaces ainsi posées à la vie privée. Ce faisant, nous introduirons également des outils d'analyse de ces enjeux développés par les nouveaux sous-champs de la philosophie de l'information, soit l'éthique des données et l'éthique des algorithmes. La seconde section adoptera une approche plus macroscopique, examinant les structures de pouvoir en place dans l'espace numérique qui exacerbent les effets négatifs de

l'utilisation massive des données sur la vie privée. Nous traiterons de la culture de surveillance, des architectures de visibilité et du concept d'infosphère de Luciano Floridi[3].

En dernière partie, nous adresserons certains des soi-disant paradoxes et solutions soulevés dans les débats moraux sur la protection de la vie privée numérique. D'abord, nous traiterons du mythe du « *privacy paradox* »[4], cette idée selon laquelle les gens disent accorder une grande importance à la vie privée, mais cèdent en revanche leurs données personnelles et n'utilisent pas de mesures pour protéger leur vie privée. Ce mythe populaire sera présenté et déconstruit, révélant la logique fautive derrière ce dernier. Sera ensuite abordée l'utilisation de la magie morale du consentement utilisée pour renoncer à sa vie privée numérique. Nous démontrerons qu'il s'agit d'une pratique viciée sans fondement moral. Enfin, ce chapitre se conclura sur un argument en faveur d'une meilleure protection de la vie privée en ligne.

En conclusion, il sera défendu que la vie privée numérique doit être mieux protégée et que de nouveaux moyens de protections doivent être mis sur pied dans l'environnement numérique; les moyens actuels étant soit insuffisants ou impossibles à assimiler par les individus. Enfin, ce mémoire invite les philosophes à poursuivre le travail théorique et normatif nécessaire pour contribuer aux débats de sociétés sur les enjeux de vie privée en contexte numérique puisqu'il reste encore beaucoup à accomplir.

[3] Luciano Floridi, « The ontological interpretation of informational privacy », *Ethics and Information Technology*, 2005, https://doi.org/10.1007/s10676-006-0001-7.

[4] Daniel J. Solove, « The Myth of the Privacy Paradox », *SSRN Electronic Journal* 89, nº 1 (2020): 1-51, https://doi.org/10.2139/ssrn.3536265.

Privacy is like an elephant, more readily recognized than described.

J.B. Young

CHAPITRE 1 : UNE DÉFINITION DU CONCEPT DE « VIE PRIVÉE »

La « vie privée » est un concept utilisé dans de multiples disciplines. Toutefois, malgré le corpus impressionnant de définitions et représentations du concept, la littérature présente peu de cohésion, à l'exception d'un constat largement partagé : tracer les contours de la vie privée n'est pas tâche facile. Même au sein des différentes disciplines, définir le concept semble chose ardue. Un exemple probant de cette difficulté conceptuelle se révèle dans le domaine juridique. En droit, discipline dans laquelle la vie privée est un concept de grande importance[5], la définition exacte de ce à quoi le concept réfère reste floue. En effet, bien que la Charte des droits et libertés de la personne[6], le Code civil du Québec[7] et de nombreux autres règlements et lois[8] y fassent référence, ces textes de loi ne fournissent aucune définition précise et exhaustive du concept. Les définitions proposées dans ces textes listent plutôt des exemples d'atteintes à la vie privée et de mécanismes de protection de la vie privée. Le sens de ce qui est entendu par « vie privée » demeure largement délimité par les cas d'application illustrant ce qui est inclus ou exclu dans les limites de ce droit. Le Code civil du Québec indique par exemple que les atteintes à la vie privée d'une personne incluent « pénétrer chez elle ou y prendre quoi que ce soit » ou encore « capter son image ou sa voix lorsqu'elle se trouve dans des lieux privés ».[9] Mais ces exemples n'offrent pas d'indication

[5] Comme le démontre notamment le droit au respect de la vie privée pleinement reconnu et consacré par de nombreuses instances juridiques au Québec et ailleurs.

[6] Charte des droits et libertés de la personne, RLRQ c C-12, art. 5.

[7] Code civil du Québec, RLRQ c CCQ-1991, art. 35 et suivants.

[8] Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1; Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1; Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1; Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5; Voir également Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, L.Q. 2021, c. 25, au terme de laquelle le Québec a choisi de s'inspirer du modèle européen en ce qui a trait à la gestion des données, soit le Règlement n° 2016/679, Réglement Générale sur la protection des données (GDPR), Journal officiel de l'Union européenne, 27 Avril 2016.

[9] Code civil du Québec, RLRQ c CCQ-1991, art. 36

claire sur ce qu'est la vie privée, sinon qu'elle est liée à l'intégrité de la propriété privée et de l'image de la personne.

Le domaine juridique n'est pas le seul à ne pas avoir circonscrit une définition pour le concept pourtant très utilisé de vie privée. La vie privée est tantôt abordée comme un droit, tantôt comme une revendication morale, un état, une capacité ou encore une valeur[10]. Elle est parfois décrite comme le fait de ne pas être importuné par autrui, ou comme l'intégrité physique d'un lieu ou d'une personne. Elle est parfois définie négativement, en opposition à la « vie publique, » ou encore envisagée comme une valeur de société dont l'importance peut être disputée. Chose certaine, aucun consensus n'existe sur la définition de ce qu'est la « vie privée », ni sur sa fonction ou sur sa valeur[11]. Au contraire, les définitions proposées sont tantôt très vagues, tantôt très étroites, et les contours et limites du concept varient d'un auteur, d'une discipline et d'une culture à l'autre.

Ce flou théorique est, selon certains, impossible à résoudre. Selon le sociologue Alan Westin, "[few] values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists"[12]. Dans les faits, ainsi que l'écrit le professeur Benyekhlef [1992], il apparaît difficile, voire impossible, d'en arriver à une définition consensuelle du droit à la vie privée » [13]. Certains remettent même en cause l'utilité d'un concept aux contours si troubles que personne ne semble avoir une idée claire de ce qu'il implique[14]. Malgré son indétermination, la plupart des théoriciens s'entendent pour dire

[10] Fabrice Rochelandet, « II Quelles justifications à la vie privée », in *Économie des données personnelles et de la vie privée*, La Découve (Paris, 2010), 128-128.
[11] Fabrice Rochelandet, « I Définition : vie privée et données personnelles », in *Économie des données personnelles et de la vie privée*, La Découve (Paris, 2010) : p.7. https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652.htm.; Gary T Marx, « Humpty Dumpty Was Wrong - Consistency in Meaning Matters: Some Definitions of Privacy, Publicity, Secrecy, and Other Family Members », *Secrecy and Society* 1, nº 1 (2016) : p.11.; Judith Jarvis Thomson, « The Right to Privacy », *Philosophy & Public Affairs* 4, nº 4 (1975) : p.295.
[12] Tom C. Clark et Alan F. Westin, « Privacy and Freedom », *California Law Review* 56, nº 3 (1968) : p.166, https://doi.org/10.2307/3479272.
[13] Anne-Marie Burns, « Compte rendu de [MARTIN MICHAUD, Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute, 1996] », *Les Cahiers de droit* 38, nº 1 (1997) : p.1.
[14] Daniel J Solove, « Privacy: A Concept in Disarray », in *Understanding Privacy* (Harvard University Press, 2008), 1-11.

que la vie privée reste un concept pertinent[15]. Il y a quelque chose de suffisamment important dans le concept de vie privée qu'il est encore aujourd'hui, et peut-être plus que jamais, un concept au centre des enjeux contemporains. Ceci est d'autant plus vrai que l'attention portée à ce concept se voit en effet renouvelée et alimentée par chacune des évolutions technologiques ayant menacé son intégrité : "maintaining privacy has gradually changed with the introduction of new technologies. The mass appearance of photographs in newspapers at the end of the nineteenth century made us experience privacy as 'the right to be let alone' (Warren and Brandeis 1890), followed in the 1960s by a focus on personal data protection as a reaction to the emergence and spread of digital data (Solove 2002)" [16]. Les avancées technologiques des dernières décennies en matière de collecte et de traitement d'informations en sont la plus récente démonstration et la protection de la vie privée se retrouve ainsi parmi les trois premiers principes de la *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, engagement social élaborant un cadre éthique pour le déploiement de l'intelligence artificielle (IA)[17].

À la lumière de l'indétermination entourant le concept de vie privée, ce chapitre a pour objectif de situer une définition de la vie privée qui servira pour la suite de notre analyse. En effet, avant de traiter de tout enjeu éthique lié au concept de vie privée, il est nécessaire de s'attarder à sa définition afin d'établir ce à quoi le concept fera référence dans le cadre de ce travail. Ce chapitre servira donc à situer le concept de vie privée parmi les différentes interprétations de ce dernier dans la littérature.

On trouve dans les débats théoriques entourant la définition de la vie privée trois points de tension récurrents. Le premier concerne la cohérence du concept de vie privée. Il distingue les réductionnistes qui conçoivent la vie privée comme une coquille vide sans réelle substance et les antiréductionnistes qui défendent au contraire qu'il s'agisse d'un concept cohérent et empreint de sens[18]. Le second débat notoire touche la portée normative plus ou moins large comprise dans les

[15] Judit Decew, « Privacy », in *Stanford Encyclopedia of Philosophy*, 2018, https://plato.stanford.edu/archives/spr2018/entries/privacy/.
[16] Olya Kudina et Melis Baş, « "The end of privacy as we know it": Reconsidering public space in the age of Google Glass », in *Surveillance, Privacy and Public Space*, 1st Edition (Routledge, 2018), p.121.
[17] Marc-Antoine Dilhac et Christophe Abrassart, « Déclaration de Montréal pour un développement responsable de l'intelligence artificielle » (Montréal: Université de Montréal, 2018).
[18] Adam Moore, « Defining Privacy », *Journal of Social Philosophy* 39, nº 3 (septembre 2008): p.413, https://doi.org/10.1111/j.1467-9833.2008.00433.x.

définitions possibles de la vie privée[19]. Alors que certains prônent des approches purement descriptives et exemptes de considérations morales, d'autres insistent sur la normativité inhérente du concept. Finalement, un troisième point de tension, moins formellement abordé dans la littérature, mérite d'être étudié. Il s'agit de l'unité d'analyse utilisée pour concevoir la notion de vie privée. La vie privée est parfois présentée comme un état de contrôle sur soi et ses informations[20], parfois comme accès plus ou moins grand à l'autre[21]. On trouve également des définitions qui adoptent une perspective différente, traitant la vie privée comme fonction d'un processus[22]. Il apparaît donc essentiel de choisir un angle d'analyse approprié pour aborder la vie privée.

Si aucune définition ne fait actuellement consensus dans la littérature déjà substantielle sur le concept de vie privée, ces trois débats permettent de se situer dans le spectre des définitions données à la vie privée. L'analyse des avantages et inconvénients des différentes positions théoriques nous permettra également de faire les choix nécessaires pour en arriver à une définition appropriée du concept de vie privée. La revue de littérature proposée dans ce chapitre débutera par une brève histoire du concept de vie privée, les fondements de cette dernière offrant un peu de contexte quant aux origines des trois débats évoqués ci-dessus. Ces derniers seront ensuite approfondis, permettant de situer le concept qui servira pour le reste du projet. Finalement, une définition de la vie privée sera proposée, inspirée de la conception processuelle d'Irwin Altman[23].

CONCEPTUALISER LA VIE PRIVÉE : UNE HISTOIRE, TROIS DÉBATS

L'objectif de cette section est de fournir un concept adapté aux besoins théoriques d'un projet s'intéressant au monde des données numériques. Toutefois, la définition proposée et les choix conceptuels effectués dans ce chapitre offrent un concept qui ne se veut pas nécessairement spécifique au contexte numérique. Si ce dernier apporte son lot d'exigences et de contraintes en ce qui a trait au choix approprié d'une définition de « vie privée » pouvant s'y appliquer, l'objectif ici est de comprendre la notion de vie privée indépendamment du contexte numérique, pour ensuite

[19] *Ibid*., 412.
[20] *Ibid*., 414.
[21] Madison Powers, « A Cognitive Access Definition of Privacy », *Law and Philosophy* 15, nº 4 (1996): p.15.
[22] Louis Sagnières, « La démocratie à l'heure de l'internat : Autonomie politique, vie privée et espace public dans un environnement numérique » (Université de Montréal, 2015) : p. 39.
[23] Irwin Altman, *The Environment and Social Behavior* (Brooks/Cole Publishing Compagny, 1975).

explorer la façon dont elle est affectée par ce contexte. La définition proposée dans ce chapitre se veut donc universelle, ou suffisamment générale pour traiter de la vie privée dans son ensemble. Elle se veut également, autant que possible, indépendante de tout contexte culturel, et pourrait en théorie s'appliquer à différentes sociétés aux normes et coutumes variées. Finalement, ce chapitre interroge la notion de vie privée indépendamment de la question d'un droit à cette dernière. En effet, définir un droit à quelque chose sous-entend que cette chose doive être protégée. Mais ne faut-il pas d'abord définir qu'est-ce cette chose avant de se demander si elle doit être protégée et dans quelle mesure ? L'intérêt, ici, n'étant pas d'élaborer une théorie du droit, mais plutôt de comprendre comment réfléchir le concept de vie privée dans le contexte de l'utilisation massive des données, c'est pourquoi ce chapitre élabore une définition du concept de vie privée, et non d'un droit à ce dernier.

La petite histoire du privé

Les origines du concept de vie privée, en tant qu'idée à fonction politique ou sociale, sont généralement associées à la séparation classique, d'abord introduite par Aristote puis reprise par John Locke et John Stuart Mill, entre la sphère dite « privée » et l'autre « publique »[24]. Dans cette conception, la sphère privée, lieu protégé du regard du reste de la société, offre la possibilité d'un refuge, d'une protection aux intrusions externes. La distinction entre ces deux sphères de vie illustre parallèlement une opposition entre la vie domestique et la vie politique, ainsi que la différence entre ce qui relève de la compétence du gouvernement et ce qui relève de l'individu en matière d'administration : le privé est la sphère dans laquelle les autorités publiques ne peuvent s'ingérer[25]. Dans le modèle libéral de la dichotomie public/privé développé aux 17e et 18e siècles, la sphère du privé est le lieu d'épanouissement des opinions et croyances personnelles, lieu sacré qui permet aux individus de développer leur pensée critique, de forger leur indépendance d'esprit et d'entretenir leur individualité, qualités nécessaires à l'exercice fondamental de la liberté politique[26]. En effet, l'espace privé permet à tout un chacun de ressourcer ses opinions à travers

[24] Rochelandet, « I Définition : vie privée et données personnelles », *op. cit*., p.7.
[25] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Standford University Press, 2010) : p.91.
[26] Guillaume Latzko-Toth et Madeleine Pastinelli, « Par-delà la dichotomie public/privé : la mise en visibilité des pratiques numériques et ses enjeux éthiques », *Tic & société [Online]* 7, no 2 (2014) : p.5. https://doi.org/10.4000/ticetsociete.1591.

l'exercice de la méditation ou de la philosophie pour ensuite revenir dans l'espace public avec des idées indépendantes de toute influence externe, notamment l'État. L'espace privé est alors bien circonscrit dans les mœurs et dans la loi : il s'agit du domaine de la propriété privée, soit de la maison[27]. La loi protégeait ainsi la demeure, empêchant quiconque, y compris le gouvernement, de s'introduire dans le domicile, lieu protégé, exempt de tout regard ou intervention étrangère[28].

Il est dit que la notion moderne de vie privée est quant à elle le fruit des réactions vis-à-vis des nouvelles technologies médiatiques popularisées à la fin du 19e siècle, notamment la photographie « instantanée », la télégraphie et l'enregistrement sonore[29]. Ces derniers outils offrent des possibilités nouvelles d'exposition de la vie quotidienne, et lancent un débat sociétal sur ce que devrait être le droit à la vie privée.[30] Ainsi, en 1890 est publié l'article de Samuel de Warren et Louis Brandeis « The Right to Privacy »,[31] considéré comme l'un des articles de revue du droit les plus influents de l'histoire américaine[32], et même comme « l'acte de naissance » de la notion moderne de vie privée[33]. Avec leur article, Warren et Brandeis intègrent une toute nouvelle dimension au concept de vie privée : " [this] privacy was, in key respects, new. It was concerned less with an individual's immediate surrounds than with image, information, biography, and what Americans were beginning to call 'personality'"[34]. Le 'right to be let alone' de Warren et Brandeis a ainsi cristallisé le passage d'une forme de vie privée fondée sur la propriété à une forme de vie privée basée sur la personne, son identité et son image. L'inquiétude occupant alors les esprits n'est en l'occurrence plus celle d'une intrusion dans la demeure par des agents gouvernementaux, mais plutôt celle de l'utilisation agressive de l'appareil photo par les photographes et journalistes,

[27] Irwin R Kramer, « The Birth of Privacy Law: A Century Since Warren and Brandeis », *Catholic University Law Review Cath. U. L. Rev* 39, nº 3 (1990) : p.705. http://scholarship.law.edu/lawreview%0Ahttp://scholarship.law.edu/lawreview/vol39/iss3/3.
[28] *Ibid*.
[29] Sarah E. Igo, *The Known Citizen : A History of Privacy in Modern America* (Harvard University Press, 2018) : p.17.
[30] *Ibid*.
[31] Samuel D Warren et Louis D Brandeis, « The Right to Privacy », *Harvard Law Review* 4, nº 5 (1890): 193-220.
[32] Kramer, *op. cit.,* p.704.
[33] Rochelandet, « I Définition : vie privée et données personnelles », *op. cit*., p.7.
[34] Igo, *op. cit*., p.19

tant d'invasions de l'intime et d'assauts contre les personnalités individuelles; ces "new machineries of exposure"[35].

Depuis ce tournant majeur dans la conceptualisation du privé, l'intérêt pour la notion s'est amplifié et la littérature sur la vie privée a foisonné dans le dernier siècle[36]. De nouvelles dimensions du privé ont ainsi émergé. La vie privée est encore parfois associée à la notion de propriété privée, mais également à celle d'autonomie, au secret ainsi qu'à la quiétude ou encore à la liberté, tant de facettes qui contribuent à l'indétermination actuelle du concept. Chose certaine, comme les derniers paragraphes le laissent entendre, la notion moderne du concept de vie privée s'est initialement vue théorisée par des juristes sous la forme d'un droit à quelque chose. Aussi l'influence de la littérature juridique sur la construction de la vie privée est sans équivoque. Le volume et l'importance de la littérature de nature juridique ne pouvant être ignorés, plusieurs auteurs abordés dans ce chapitre traitent la vie privée comme Warren et Brandeis, soit à titre de « droit »[37]. Plusieurs conceptions provenant du champ juridique seront étudiées dans le cadre de ce chapitre, bien que ce dernier ne s'intéresse pas au droit à la vie privée, comme mentionné précédemment.

À la lumière de ces remarques préalables sur les origines historiques de la vie privée, nous pouvons maintenant attaquer les trois grands débats entourant le concept dans la littérature des dernières décennies, commençant avec le plus fondamental, à savoir celui qui conteste la pertinence même du concept de vie privée.

Existe-t-il réellement une chose telle que « la vie privée »?

Voici ce que remettent en cause certains auteurs : y a-t-il vraiment une chose identifiable et singulière qui soit le propre de ce que l'on appelle « vie privée »? Devant le problème entourant la définition du concept de vie privée, plusieurs auteurs adoptent en effet une position réductionniste ou taxonomiste[38]. Ils défendent que, s'il est aussi difficile d'en arriver à une définition cohérente et unifiée du concept de vie privée, c'est tout simplement parce qu'il n'y en a

[35] *Ibid*.
[36] Decew, *op. cit*.
[37] Les deux auteurs réfèrent en effet au « right to be let alone » dans leur article dont le titre rappelle encore une fois l'angle théorique juridique adopté dans « The Right to Privacy ». Voir Warren & Brandeis, *op cit*.
[38] Powers*, op. cit*.

pas! Les réductionnistes les plus « extrémistes » vont jusqu'à proposer d'abandonner complètement le concept. C'est le cas de Judith Jarvis Thomson dans son article « The Right to Privacy » lorsqu'elle écrit: "[perhaps] the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is"[39]. Cette citation se trouve à la première phrase de l'article écrit par Jarvis Thomson en 1975, dans lequel elle défend que le droit à la vie privée soit en fait une coquille vide dont chaque élément renvoi en fait à d'autres droits plus fondamentaux.

Pour convaincre son lecteur, Jarvis Thomson aborde méthodiquement une dizaine d'exemples mettant en lumière des problématiques usuellement liées au droit à la vie privée. Pour chacun d'eux, elle met en évidence la faute qui est en jeu et en vertu de quel droit il s'agit effectivement d'une faute. Par exemple, illustre-t-elle, le fait de posséder une photographie donne à un individu le droit positif de jouir de cette dernière, de la regarder ou encore de la déchirer s'il lui en prend l'envie. En contrepartie, le droit de propriété impose des « droits négatifs » (des obligations) aux autres : ne pas regarder ou déchirer la photographie sans le consentement du propriétaire par exemple[40]. Ainsi, si une personne regarde, s'empare, ou déchire la photographie contre le gré de son propriétaire, elle pose un tort à celui dont l'objet est la propriété.

Au fil de ses exemples, Jarvis Thomson fait la démonstration que, dans chaque cas présenté, l'enjeu au centre de la problématique découle en fait d'un enjeu autre que celui de la vie privée. Par exemple, dans le cas présenté ci-dessus, ce n'est pas le droit à la vie privée, mais bien celui à la *propriété* qui serait en cause selon Jarvis Thomson. Dans cette conception, le seul tort découlant du fait du subtiliser quelque chose à autrui (une photographie par exemple), est de prendre quelque chose qui ne nous appartient pas. La question à savoir si la personne désirait garder quelque chose privé, soit loin du regard d'autrui, et qu'il s'agit en ce sens non seulement d'un vol, mais également d'une intrusion est complètement ignorée par Jarvis Thomson. De la même façon, fouiller ou toucher quelqu'un est une atteinte à l'intégrité physique lorsque cette personne n'y consent pas, un vol d'identité affecte la liberté et l'autonomie d'une personne, etc. Jarvis Thomson en vient ainsi à conclure : "[for] if I am right, the right to privacy is "derivative" in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy"[41]. D'après elle, ce qu'on nomme communément

[39] Jarvis Thomson, *op. cit*., p. 295.
[40] Jarvis Thomson, *op. cit*., p.300
[41] Jarvis Thomson, *op. cit*., p.313

le « droit à la vie privée » est tantôt un dérivé du droit à la propriété, tantôt du droit à la liberté ou du droit à l'autonomie, bref il ne possède selon elle aucune caractéristique suffisamment exclusive ou spécifique qui justifie d'en faire un droit à part entière. Jarvis Thomson en vient à la conclusion que si l'on peut réduire le droit à la vie privée à un dérivé d'autres droits, alors le droit à la vie privée n'a plus d'utilité. En effet, si le droit à la vie privée se résume à un amalgame d'autres droits, qui sont eux plus directement liés aux torts en cause, pourquoi donc poursuivre l'usage de celui qui est simplement dérivé des droits fondamentaux?

La force de l'argument réductionniste défendu par Jarvis Thomson a depuis été remise en cause à plusieurs reprises. On dénote d'abord certaines incohérences logiques dans son argument. Jarvis Thomson soutient que le droit à la vie privée dérive d'autres droits comme celui à la propriété. Or, si un droit découle effectivement d'un autre, il n'est pas si évident de déterminer lequel des deux précède l'autre. Qu'est-ce qui prouve que ce ne serait-ce pas plutôt le droit à la propriété qui découle du droit à la vie privée? Si le droit à la vie privée est lié au droit à la propriété privée, le sens de la relation entre ces différents droits n'est pas évident. Il est en effet possible de prendre l'exemple de Jarvis Thomson et d'en faire la démonstration inverse. Si la vie privée est par exemple conçue comme la possibilité pour les personnes de limiter l'accès des autres à elle, alors il est concevable que le droit de propriété privé découle en fait d'un droit à la vie privée et non l'inverse[42]. Bref, le sens de la soi-disant dérivation conceptuelle à la base de l'argument de Jarvis Thomson est questionnable et demanderait probablement une longue analyse sociohistorique pour être démystifié.

De plus, si le droit à la vie privée emprunte effectivement des éléments dérivés d'autres droits, un second argument logique peut être tout de même être opposé à Jarvis Thomson. Cette dernière suppose qu'un ensemble d'éléments dérivés d'autres droits (la propriété, l'intégrité physique, la liberté) ne peut former un tout cohérent (la vie privée). Pourtant, si nous avons un premier droit A composé de l'ensemble cohérent de « sous-droits » a^1, a^2 et a^3; un deuxième droit B composé de b^1, b^2 et b^3, l'ensemble cohérent a^1, b^2 et c^3 peut très bien composer un troisième droit distinct C. Il reste maintenant à savoir si le tout cohérant 'C' est un concept utile en soit.

Il n'est dans tous les cas pas surprenant de voir plusieurs concepts se chevaucher comme la liberté et l'autonomie par exemple. Judith Wagner DeCew rappelle qu'il est normal que les

[42] Jeffrey H Reiman, « Privacy, Intimacy, and Personhood », *Philosophy & Public Affairs* 6, nº 1 (1976): p. 27.

concepts de vie privée et de liberté partagent autant de similitudes considérant l'association historique entre le droit à la vie privée et "the right to be let alone", ce dernier étant "the well-known explanation of a concept of negative liberty in terms of freedom from interference"[43]. Mais la vie privée et la liberté peuvent très bien partager certaines composantes communes sans pour autant que l'une ou l'autre soit une simple dérivation de la première. Reiman souligne "even if privacy rights were a grab-bag of property and personal rights, it might still be revealing, as well as helpful, in the resolution of difficult moral conflicts to determine whether there is anything unique that this grab-bag protects that makes it worthy of distinction from the full field of property and personal rights"[44]. Ainsi, il importe peu si la vie privée découle du principe de propriété, ou vice versa. Si les thématiques et enjeux soulevés par le concept de vie privée sont suffisamment intéressants et spécifiques, alors cela semble suffisant pour en faire un concept digne d'intérêt.

En plus de ces dernières erreurs logiques, une autre faiblesse de l'argumentaire de Jarvis Thomson est soulevée par l'auteur William Parent. Dans les exemples fournis par Jarvis Thomson, elle suggère à chaque fois qu'il ne s'agit pas d'un enjeu spécifique à la « vie privée », et propose tour à tour un autre « droit » qui serait plus à même d'exprimer l'enjeu moral ou légal de son exemple. Or remarque Parent, plusieurs des droits qu'elle propose sont assez invraisemblables :

> Thomson's attempt to diminish the status of the right to privacy fails to persuade. It requires that we recognize a plethora of rights whose status is certainly more problematic than that of the right whose significance she wants to impugn. Do we really think of ourselves as possessing the rights not to be looked at and listened to? Must we talk about a right not to have our property looked at? Thomson's claim that we waive these rights all the time - a claim she has to make to avoid the absurd implication that our rights are violated thousands of times every day- flies in the face of common sense and common experience. Just ask whether you thought of yourself as having waived the right not to be listened to before speaking with people today. The idea seems preposterous.[45]

Aussi, si l'on fait abstraction de ces supposés « sous-droits » que Jarvis Thomson propose, la liberté et la propriété privée n'offrent pas d'explication satisfaisante pour exprimer en quoi certains de ses exemples sont problématiques. Si quelqu'un est invité chez des amis et que cette personne

[43]Judith Wagner Decew, « The Scope of Privacy in Law and Ethics », *Law and Philosophy*, Springer, 5, nº 2 (1986): p.162., Voir également la section *La petite histoire du privé.*

[44] Reiman, *op. cit*., p.28

[45] W A Parent, « Privacy, Morality, and the Law », *Philosophy & Public Affairs* 12, nº 4 (1983): p.279.

pendant la soirée s'introduit dans une chambre à coucher pour aller regarder les sous-vêtements et autres effets personnels, elle ne brime en rien la liberté des hôtes. Et dans la mesure où *ne pas regarder* le bien d'autrui ne peut pas être raisonnablement considéré comme un des droits négatifs associés à la propriété privée, le caractère abusif de cette intrusion doit trouver sa source ailleurs[46]. Le réductionnisme de Jarvis Thomson paraît ainsi injustifié et il apparaît justifier de proposer qu'il y ait quelque chose de suffisamment spécifique et unique dans le concept de vie privée pour qu'il se distingue des notions de liberté et de propriété pour qu'il ne puisse être simplement réduit à ces deux dernières notions.

Trente ans après l'article de Jarvis Thomson, Daniel Solove propose pour sa part une approche que l'on pourrait qualifier de taxonomiste, ou de réductionniste faible. Il part également du constat selon lequel les problèmes concernant la vie privée sont fréquemment mal interprétés[47]. Cette confusion s'explique d'après lui parce que la vie privée désigne un large éventail de choses disparates et donc ne désigne rien de particulier. En d'autres termes, il n'y a rien de spécifique ou de propre à la vie privée : c'est un amalgame de problèmes avec certaines similarités. Il en vient à la conclusion que "the attempt to locate the "essential" or "core" characteristics of privacy has led to failure"[48] et propose, au lieu de poursuivre la recherche à son avis vaine d'une seule définition cohérente, d'adopter une approche alternative et novatrice pour aborder la vie privée. Solove s'inspire de la notion d'« air de famille » de Ludwig Wittgenstein, proposant que certains concepts n'ont pas une seule ou quelques caractéristiques fondamentales, mais qu'ils puisent plutôt dans un ensemble d'éléments similaires : "[privacy] therefore consists of many yet different related things"[49]. Son approche taxonomiste prend des cas particuliers de problèmes de vie privée et conceptualise cette dernière comme l'ensemble des éléments qui se retrouvent dans ses différents cas, ces éléments ayant certains points communs, mais dont il est impossible de rendre compte en fonction d'une seule et même caractéristique. Cela permet selon Solove de mieux identifier toutes les occurrences de violation du droit à la vie privée. Adam Henschke, qui partage lui aussi cette vision taxonomiste, l'explique ainsi :

[46] Moore, *op. cit*.
[47] Solove, "Privacy: A Concept in Disarray", *op. cit*., p.6.
[48] *Ibid*., p.8.
[49] *Ibid*., p.9.

> More than simply offering plural meanings, seeing privacy as a cluster allows the different elements to both explain and limit each other. The point here is that the problem with the different conceptions viewed so far is that, in seeking to reduce privacy to a single conception, they lose the utility of the other conceptions. My point is that rather than looking for 'the one true meaning of privacy,' we should instead look to the different elements that each conception brings to privacy discussions. Importantly, we recognise that in some situations, certain conceptions will be more relevant, others less so.[50]

Si elles se veulent moins réductionnistes que celle de Jarvis Thomson, les approches taxonomistes de Solove et Henscke, ne sont au final guère différentes et se heurtent aux mêmes contre-arguments. En effet, si la vie privée consiste effectivement en un ensemble d'éléments semblables, mais différents, sans dimension ou caractéristique propre à une définition cohérente de la vie privée, alors la théorie de Solove vient vraisemblablement renforcer l'argument de Jarvis Thomson selon lequel la vie privée est une coquille vide renvoyant à d'autres concepts. Il ne fait que défendre, contrairement à Jarvis Thomson, que cette coquille soit utile. Or l'utilité d'un concept sans définition claire ni substance propre semble limitée et les approches réductionnistes et taxonomistes également.

Ainsi, devant la faiblesse des arguments réductionnistes et leur incapacité à expliquer pourquoi les problèmes généralement associés au concept de vie privée sont liés les uns aux autres, on suit l'hypothèse des théoriciens qui s'entendent pour dire qu'il y a quelque chose qui est à la fois unique et important dans le concept de vie privée - même s'ils ne s'entendent pas sur quelle est cette chose exactement. Suivant cette intuition, les approches réductionnistes ne sont pas retenues pour les fins de ce mémoire bien qu'elles aient permis de mettre en lumière le degré de complexité et de diversité contenu dans le concept de vie privée. Les prochaines sections explorent des approches offrant des définitions non réductionnistes de la vie privée, avec la conviction qu'elles pourront mettre en lumière une définition du privé à la fois cohérente et distincte de celles des concepts de liberté et d'autonomie. Un second débat de la littérature, opposant les conceptions normatives aux approches descriptives de la vie privée, permet de situer le concept de vie privée.

[50] Adam Henschke et On Privacy, « On Privacy », in *Ethics in an Age of Surveillance* (Cambridge: Cambridge University Press, 2014), 28-55, https://doi.org/10.1017/9781316417249.002.

Un concept chargé de normativité : vers une définition descriptive de la vie privée

La vie privée est un concept chargé de normativité. Judith Wagner DeCew souligne l'importance de cette caractéristique du privé. Il s'agit selon elle d'une notion conventionnelle et relative[51]. Conventionnelle, parce que construite socialement, et donc alimentée par les normes et conventions sociales, par les us et coutumes. Relative, parce que variant selon les époques, les sociétés, les groupes et les individus. La conception de la vie privée et de ce qui y est associé est largement transmise socialement et culturellement et peut varier à travers le temps et l'espace.[52] On peut par exemple penser à la religion, qui fut à une époque pratiquée de façon très publique et qui est aujourd'hui devenue dans beaucoup de sociétés libérales un objet relégué au privé, voir bannie de la sphère publique jusque dans une certaine mesure.[53] Sa perspective ancrée dans une approche sociologique conduit DeCew à lier la définition de la vie privée à ce qui est socialement considéré comme privé. Elle indique "the realm of the private [is] whatever is not generally, that is, according to a reasonable person under normal circumstances, or according to certain social conventions, a legitimate concern of others because of the threat of scrutiny or judgment and the potential problems following from them"[54].

Deux remarques s'imposent ici. D'abord, plutôt que de développer une définition théorique de ce que pourrait être un concept vie privée, DeCew donne une définition positive, basé sur l'observation empirique de ce qu'est définit comme étant privé dans le monde. La vie privée est l'ensemble des choses, endroits ou informations qui sont généralement considérés comme étant privés dans une société ou par une personne raisonnable. Ce premier élément ancre sa définition dans une normativité sociale, soit celle des normes et conventions en place dans cette société donnée. Aussi cette détermination par la norme de la vie privée fait de cette dernière un concept tout aussi contextuel : on devra définir la vie privée pour chaque contexte social particulier. Ensuite, la définition de DeCew introduit un second degré de normativité en sous-entendant que ces éléments sont « légitimement » du domaine privé de par les normes sociales en place – qui en font des sources de jugement. Il s'agit effectivement d'une conception normative du privé puisqu'elle inclut une revendication morale dans la définition même du concept. Ce faisant,

[51] DeCew, « The Scope of Privacy in Law and Ethics », *op. cit*., p.150.
[52] DeCew, « The Scope of Privacy in Law and Ethics », *op. cit*., p.150.
[53] Loi sur la laïcité de l'État, RLRQ c L-0.3
[54] Decew, « The Scope of Privacy in Law and Ethics », *op. cit*., 172.

DeCew répond en quelque sorte à la question « qu'est-ce que la vie privée ? » par « c'est ce qui *devrait* être privé », et à « qu'est-ce qui devrait être privé », par « c'est ce qui est socialement considéré comme étant privé ». C'est ainsi qu'on commence peu à peu à discerner un certain sophisme naturaliste dans la définition de DeCew qui glisse entre le jugement de fait et le jugement de valeur.

Helen Nissenbaum adopte une approche similaire à celle de DeCew, mettant en évidence que les attentes et conceptions des personnes en matière de vie privée se développent quotidiennement à travers le contexte des structures sociales en place et évoluant dans le temps.[55] Elle définit la vie privée comme suit : "a right to live in a world in which our expectations about the flow of personal information are, for the most part, met"[56]. Pour Nissenbaum, les attentes en matière de vie privée se développent dans le contexte des structures sociales dont nous faisons l'expérience au quotidien. À la différence de DeCew, la conception de la vie privée de Nissembaum se concentre sur le contrôle de la circulation d'information uniquement. Mais le raisonnement derrière la définition est le même : le contexte social et les pratiques existantes donnent un cadre de référence aux individus sur ce qui peut être attendu de façon raisonnable[57] en termes d'accès aux informations personnelles. Malheureusement le problème dans la définition est également le même. Marcel Becker l'exprime ainsi : "referring to existing practices to find ultimate normative justification is not a good strategy"[58]. En effet, prendre comme point de référence les pratiques en place pour justifier ce qui est légitime fait plomber la menace d'un conservatisme rigide. Ce n'est pas parce qu'une chose est en place et socialement acceptée ou encouragée que cette chose est nécessairement éthique, morale ou même légitime. Aussi le danger du conservatisme est encore plus réel dans le contexte d'un monde susceptible de faire face à de nombreux changements et à une évolution rapide - technologique en l'occurrence – souligne Becker :

> The revolution in techniques of surveillance makes almost all information that is in plain view information. Any development in surveillance or monitoring, if

[55] Nissenbaum, *op. cit.*, p. 129-137.
[56] *Ibid.*, p.231.
[57] La notion d'attente raisonnable doit ici être comprise à la lumière de la tradition jurisprudentielle.
[58] Marcel Becker, « Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy », *Ethics and Information Technology* 21 (juillet 2019): p.313, https://doi.org/10.1007/s10676-019-09508-z.

> communicated well, might be placed under the umbrella of reasonable expectation. Suppose a government takes highly questionably measures (for instance, it collects all metadata on phone calls) and is completely honest about doing so. The government does not want to surprise its citizens, so it duly informs the public that this is how things are being done. Anyone who makes a phone call has the expectation that her data will be stored. [59]

Les nouvelles technologies changent l'impact des règles et pratiques en place. Ces dernières peuvent rapidement devenir désuètes et doivent être repensées. Bref, si les attentes raisonnables des individus en matière de vie privée, mobilisées pour offrir une définition de ce qu'est et de ce que devrait être la vie privée, sont basées sur des normes et des pratiques viciées, on se retrouve dans un modèle conservateur, basé sur l'observation des normes dans lequel ce qui était fait avant justifie ce qui sera fait ensuite. De plus si la vie privée se résume aux attentes socialement partagées, alors le danger de dérives comme celle illustrée par Becker devient imminent. Facebook et Google ont d'ailleurs largement profité de ce principe en habituant leurs usagers à n'avoir absolument aucune attente en matière de vie privée[60].

Les constats de DeCew et Nissenbaum sur le caractère socialement construit de la vie privée mettent de l'avant une composante importante du concept de vie privée : soit que ce concept est ancré dans le social et que ses représentations sont sujettes à une évolution organique dans les sociétés. Cependant, le cadre normatif basé sur la validité du contexte social que cette approche offre n'est pas satisfaisant. En fait certains auteurs rejettent complètement les approches normatives de la vie privée, y voyant une source de confusion supplémentaire. C'est notamment le cas de Parent qui reproche aux définitions normatives de confondre la définition du privé avec celle d'un droit à la vie privée justement. Pour lui, une bonne définition doit décrire les conditions objectives en vertu desquelles il y a ou non vie privée. Il propose cette définition : "privacy is the condition of not having undocumented personal knowledge about one possessed by others"[61]. Selon sa définition, lorsqu'une personne n'a pas d'informations personnelles[62] sur elle en possession d'autrui, alors, elle jouit de vie privée et on peut identifier une perte de vie privée

[59] Becker, *ibid*.
[60] *Ibid*.
[61] Parent, *op.cit*., p.269.
[62] Paradoxalement, Parent donne tout de suite après une définition non objective de ce qui constitue les informations personnelles indiquant que « [they] consist of facts about a person which most individuals in a given society at a given time do not want widely known about themselves » (Voir Parent, *op.cit*., p.269).

lorsque de l'information sur elle est acquise par une autre personne. Mais cette perte de vie privée n'est pas nécessairement synonyme de violation d'un droit moral ou légal à la vie privée, d'où l'importance d'en différencier les définitions selon Parent.

L'attrait des définitions descriptives est qu'elles permettent de comprendre la vie privée sans poser de jugement sur sa valeur ou sa désirabilité. Alors que les définitions normatives intègrent des revendications morales, les définitions descriptives s'en tiennent à identifier les conditions objectives du privé. Madison Powers, qui défend également les mérites d'une approche descriptive, explique : "a purely descriptive definition would not entail any normative judgments about whether privacy is a good or valuable condition which ought to be preserved, […] the aim of a descriptive definition is to specify what a loss of privacy consists in, independent of whether it is wanted or unwanted, intentional or inadvertent, ill-motivated or well-meaning, or of substantial or minimal significance from a moral or legal perspective"[63]. Or en définissant uniquement les conditions de la vie privée, cela permet d'identifier objectivement quand il y a une perte ou une diminution de vie privée, sans égard ni à la cause, ni au bien ou au mal de cette perte. Peu importe si cette perte est survenue par inadvertance (un couple à la fenêtre ouverte dont la dispute est entendue par un passant), de façon intentionnelle (une personne écrit et publie une lettre ouverte sur une expérience personnelle), ou encore par le résultat d'actes malveillants (un vol d'identité pour fins de fraude). Et peu importe aussi si cette perte est par la suite jugée bénéfique ou néfaste : une personne peut très bien vouloir dévoiler des informations sur elle-même ; toute perte de privé n'est pas automatiquement problématique. Ainsi, selon Madison et Parent, la seule question à laquelle devrait répondre la définition de la vie privée est « *qu'est-ce qui constitue une perte de vie privée ?* », sans poser de jugement sur ce qui devrait être privé ou non.

La capacité d'observer et évaluer objectivement les caractéristiques d'un objet avant de porter un jugement sur sa valeur ou les impératifs qui lui sont liés donne un avantage certain en termes de clarté et évite toute confusion normative. Elle laisse ouverte la possibilité que dans certaines circonstances, une diminution du niveau de vie privée puisse être positive. On propose donc à la suite de Madison et Parent de cerner la vie privée de façon objective, d'en comprendre la mécanique d'abord, pour ensuite construire les arguments moraux nécessaires sur son importance ou les besoins en matière protection de celle-ci. Il faut donc une définition qui fournit

[63] Powers, *op. cit*., p.374.

des critères suffisamment objectifs pour permettre d'identifier adéquatement ce qu'est la vie privée. Une bonne définition devrait également rendre compte de la complexité du domaine privé, tantôt relatif, d'une personne ou d'un groupe à l'autre, tantôt conventionnel, puisque souvent établi par les normes particulières des différentes sociétés[64].

La définition de Parent, aussi descriptive soit-elle, n'est toutefois pas retenue. Malheureusement, l'avantage simpliste de sa définition en fait également le défaut : en définissant un critère objectif à la vie privée qui est circonscrit aux informations personnelles sa définition s'avère trop étroite, ignorant certains aspects essentiels du privé. Parent, rappelons-le, propose une définition strictement informationnelle du privé : "privacy is the condition of not having undocumented personal knowledge about one possessed by others"[65]. En faisant du privé uniquement une question de possession d'informations personnelles, il exclut en effet tous les autres types d'intrusions comme les intrusions physiques ou technologiques. Selon sa définition, mettre sous écoute un téléphone n'est pas en soi une violation de la vie privée. Il s'agirait plutôt d'une atteinte à la liberté ou à l'autonomie de l'individu, mais pas à la vie privée[66]. La perte de vie privée ne serait effective qu'à partir du moment où il y aurait une information personnelle obtenue via cette intrusion. Ce critère très précis de ce qui constitue une perte de vie privée est plutôt limité. Au sens de plusieurs auteurs, il existe de multiples autres types de violations en lien avec la vie. DeCew note que :

> [It] is widely recognized that others' physical access to one can limit one's privacy in other ways as well. Ruth Gavison has argued that one can lose privacy merely by becoming the object of attention, even if no new information becomes known and whether the attention is conscious and purposeful, or inadvertant. More obviously, one's privacy is diminished when others gain physical proximity to them, as Peeping Toms for example, through observation of their bodies, behavior, or interactions, through entry into a home under false pretenses, or even by a move from a single-person office to a shared one.[67]

Les données étant au cœur du monde numérique, ce focus sur l'informations pourrait paraître adéquate. Pour un projet centré sur les données massives, l'accès aux informations

[64] DeCew, « The Scope of Privacy in Law and Ethics », *op. cit*. p.150.
[65] Parent, *op. cit*., p.269.
[66] *Ibid*., p.285-286.
[67] DeCew, « The Scope of Privacy in Law and Ethics », *op. cit*., p.156.

personnelles est évidemment un enjeu majeur. Néanmoins, cette définition semble passer à côté d'éléments essentiels à la vie privée. Une personne en situation d'itinérance qui vit dans la rue, exposée au regard d'autrui, mais au sujet de laquelle personne n'a d'information, est-elle réellement dans une meilleure situation de vie privée qu'une personne qui partage de l'information sur elle à ses amis et collègues, mais qui rentre chaque soir dans une maison où elle peut faire et être à l'abri des regards indiscrets? Il semble y avoir quelque chose de plus subtil et complexe dans le concept vie privée que la seule question d'avoir de l'information sur nous soit connue d'autrui. En effet, comme la prochaine section le démontre, le problème dans la définition proposée par Parent, ne réside pas uniquement dans son étroitesse, mais également dans la façon même dont elle aborde le concept de vie privée.

Choisir une unité de référence pour parler de la vie privée

On peut penser la vie privée de plusieurs façons. On peut considérer la vie privée comme l'ensemble des choses qui sont tenues comme privées. Mais la vie privée ne se résume pas uniquement à son contenu, il y a également pour ainsi dire son contenant, c'est-à-dire les façons dont elle s'exerce, les relations entre les personnes et les processus par lesquels les gains et pertes en matière de vie s'opèrent… La faiblesse de plusieurs approches du concept de vie privée réside dans le type d'analyse qu'elles utilisent pour aborder la vie privée. Cette section montre les limites des conceptions circonscrites au contenu du privé, l'intérêt de celles basées sur les relations sociales, puis propose une définition avec une approche processuelle de la vie privée.

Dans le modèle libéral de la dichotomie publique/privée développé aux XVIIe et XVIIIe siècles et synthétisé en 1890 par la définition de Warren et Brandeis 'the right to be left alone'[68], la sphère du privé est conçue comme le lieu d'épanouissement des opinions et croyances personnelles. Un lieu sacré qui permet aux individus de se développer et d'entretenir l'individualité nécessaire à l'exercice fondamental de leur liberté politique[69]. En effet, l'espace privé permet à tout un chacun de ressourcer ses opinions à travers l'exercice de la méditation ou de la philosophie pour ensuite revenir dans l'espace public avec des idées indépendantes de toute influence externe, notamment l'État. Cette tradition a lié le concept de vie privée à la notion d'autonomie dans un paradigme centré sur les droits et libertés individuelles. Quand Parent affirme que la vie privée

[68] Becker, *op. cit*., p.308.
[69] Latzko-Toth & Pastinelli, *op. cit.*, p.5.

consiste à ne pas voir ses informations personnelles entrer en possession d'autrui, il s'inscrit dans cette tradition, faisant du privé la propriété d'un état d'accessibilité à la personne : soit quelqu'un est en possession d'informations personnelles sur moi, soit il ne l'est pas[70]. Toute une branche de la littérature conçoit le privé à partir de cette notion d'accès. D'après cette conception, une personne jouit de vie privée lorsqu'elle est capable de limiter l'accès que les autres ont à elle ou à certains aspects de sa personne, ses informations personnelles, son corps, etc. Cette approche du privé positionne le privé comme une expérience individuelle. Selon une définition basée sur l'accès, comme celle de Parent et plusieurs autres, être complètement inaccessible aux autres humains serait l'idéal de la vie privée.

Cette conception est déficiente à plusieurs égards. Le principal argument qui lui est opposé est celui de la vie partagée[71]. Il paraît en effet étrange de dire que l'intimité partagée avec ses proches constitue une perte de vie privée. Est-ce que partager de l'information avec sa famille et ses amis constitue une perte de vie privée? Le problème avec ces conceptions basées sur l'accès est le niveau d'analyse individuel qu'elles utilisent pour aborder la vie privée. Il s'agit d'une approche inadaptée à la prise en compte des relations sociales qui se révèlent centrales au concept de vie privée. L'importance de la relation sociale pour conceptualiser la vie privée est bien illustrée par l'expérience de pensée du naufragé utilisée par Fried (1968) pour critiquer les limites de la notion d'accès en matière de vie privée[72]. Il imagine un naufragé qui se retrouve seul sur une île déserte et demande s'il est exact de dire que cet exilé jouit malgré ses autres malheurs d'une parfaite vie privée. On a tendance à partager l'intuition de Fried et répondre que non, puisque le concept de vie privée ne semble pas pertient dans le cas du naufragé. L'argument avancé est que si le niveau de vie privée d'une personne est dépendant du niveau d'accès qu'on les autres à celle-ci, comme le suggère les définitions basées sur la notion d'accès, alors une situation parfaite de vie privée serait d'être complètement inaccessible. Or comme le montre l'expérience de pensée du naufragé, la notion de vie privée exige un contexte dans lequel plusieurs personnes sont en relation,

[70] Pour Parent la vie privée est un ensemble défini pour chaque personne; l'ensemble des informations personnelles de cette dernière et on peut calculer le niveau de vie privée d'une personne selon l'intégrité de cet ensemble : « a person's privacy is diminished exactly to the degree that others possess this kind of knowledge about him » (Voir Parent, *op. cit*., p.269) .

[71] Sagnieres, *op. cit*., p.37.

[72] *Ibid.,* p. 36.

sans quoi il devient simplement absurde de parler de vie privée. Rompant avec le modèle individuel classique, on fait l'hypothèse qu'il est possible de conjuguer vie privée et intimité.

Une seconde faiblesse des définitions basée sur l'accès est qu'elles n'arrivent pas à exprimer que l'intrusion seule, même sans succès, est à elle seule une atteinte à la vie privée. En effet, selon les définitions basées sur l'accès, la vie privée d'une personne est diminuée à partir du moment où autrui accède à sa personne ou des éléments de cette dernière – ses informations personnelles dans le cas de Parent. Tant et aussi longtemps que les personnes n'ont pas accédé à la personne, la vie privée est préservée. Or, il semble que la seule tentative d'intrusion suffise pour qu'il soit possible de parler d'atteinte à la vie privée. La justice québécoise avance également qu'il n'est pas nécessaire d'obtenir une information confidentielle pour brimer la vie privée. Dans cet arrêt de la Cour d'appel du Québec, les honorables juges Gendreau, Fish et Robert infirment un jugement de première instance qui avait jugé que « l'enregistrement illégal d'une conversation téléphonique ne contrevient pas en soi au droit à la vie privée » [73]. D'après eux, au contraire « [on] peut difficilement envisager une violation qui soit aussi grave et flagrante à la vie privée […] en ce que l'on a utilisé des moyens électroniques pour capter des conversations téléphoniques privées »[74]. Bref, nul besoin que les éléments considérés comme privés soient rendus accessibles pour qu'il y ait atteinte à la vie privée selon leur interprétation de cette dernière même si l'objet de convoitise n'est pas atteint. En d'autres termes, si l'on devait imaginer la vie privée comme des barrières protégeant des objets, une atteinte à la barrière elle-même peut constituer une atteinte à la vie privée.

Il faut donc trouver une définition de la vie privée qui admette la possibilité d'entretenir des rapports sociaux privilégiés avec d'autres personnes et qui rende non seulement compte du contenu du privé, mais également des mécanismes de protection de ce dernier; son contenant. Pour ce faire, un autre degré d'analyse est proposé à la suite d'Irwin Altman et Louis Sagnieres selon qui le niveau ontologique adéquat pour rendre compte du concept de vie privée est le processus. Ce que ce changement de perspective suggère, c'est que l'élément important, ou intéressant dans le concept de vie privée ne concerne pas que les éléments qu'elle garde privés, mais la façon dont ces éléments sont gardés privés. Altman propose la définition suivante : *« privacy is a central*

[73] Mascouche (Ville) c. Houle, 1999 CanLII 13256 (QC CA).
[74] *Ibid.*

regulatory process by wich a person (or a group) makes himself more or less accessible and open to others »[75]. La vie privée, en d'autres termes, est le résultat de l'ensemble des structures, mécanismes et méthodes qui rendent une personne ou un groupe de personnes moins accessibles. La question n'est donc pas qu'est-ce qui devrait être considéré comme privé, que ce soit les informations personnelles ou un espace délimité comme la maison, c'est plutôt qu'est-ce qui permet la protection de ces objets, quels qu'ils soient. La vie privée, c'est ce qui permet aux personnes de préserver certains choses ou aspects d'eux-mêmes dans un cercle d'intimité privilégié, quelles que soient la dimension de ce cercle, la nature des choses gardées privées ou les personnes avec lesquelles ces choses sont partagées.

Premier constat sur cette nouvelle définition : on note que la notion d'accès est toujours présente. Toutefois, l'accessibilité ici n'est plus le critère ultime du privé, elle est un facteur dialectique d'ouverture et de fermeture dépendant des processus de régulation en place. L'accès est encore une dimension centrale de cette définition, mais elle n'est plus conçue le critère binaire d'avoir ou non accès, d'être ou ne pas être accessible. Pour mieux exprimer cette subtilité, Louis Sagnières propose le néologisme « privatie » qui introduit « une distinction importante que le français ne peut pas faire, mais que l'anglais fait sur le plan conceptuel, mais pas lexical, entre ce qui nous permet de jouir d'une vie privée, et la vie privée dont on jouit; c'est-à-dire, entre ce qui permet l'existence du privé, et ce qui relève du privé » [76]. En effet, la traduction littérale de l'expression anglaise « I need a little privacy » qui devrait être « j'ai besoin d'un peu de vie privée » ne revêt pourtant pas exactement la même signification qu'en anglais. L'expression anglaise réfère vraisemblablement dans ce cas au contexte ou à l'état particulier de la personne à l'instant où elle émet le commentaire alors que la « vie privée » semble faire référence à quelque chose de beaucoup plus général ou diffus. Dans la phrase « *this room offers great privacy* », la traduction exacte ne serait pas « cette pièce offre beaucoup de vie privée » puisque le terme *privacy* réfère aux caractéristiques de la pièce qui participe à la vie privée. La *privacy* permet d'exprimer les conditions qui participent à la réalisation de la vie privée. Par suite, la vie privée est la situation d'une personne possédant les processus de *privacy* nécessaires pour contrôler adéquatement l'accès à sa personne. Ainsi, si l'objectif et l'effet des processus sont de réduire l'accessibilité, la

[75] Altman, *op. cit.*, p.3.
[76] Voir Sagnières, *op. cit.*, p.33, note de bas de page 11.

condition d'inaccessibilité n'est pas garante de la vie privée. Si une personne vit dans un bunker possédant toutes les technologies de *privacy* imaginables, mais qu'en raison d'une brèche a été momentanément épiée, elle a tout de même globalement plus de vie privée qu'une personne vivant dans une tente, mais à laquelle personne n'a encore fait attention.

Les processus de *privacy* permettent aux personnes de se rendre plus ou moins accessibles. À noter que le niveau de vie privée n'est pas nécessairement diminué parce qu'une personne se rend plus accessible à quelqu'un d'autre, à son partenaire par exemple. En effet, les processus de vie privée sont dirigés, ils érigent des frontières vis-à-vis du monde extérieur, mais peuvent très bien servir à protéger une intimité partagée avec autrui, ce pour quoi la définition mentionne le groupe. Quelqu'un peut avoir énormément de vie privée, soit de nombreux processus de *privacy* en place, et multiples relations d'amitié et d'amour également protégées par certaines de ces barrières. On pourrait illustrer la vie privée comme les couches d'un oignon qui en préserve le germe : chaque barrière constitue un niveau de proximité différent, certaines relations étant plus proches du centre que d'autres. La vie privée est ce qui permet de réguler le flux d'information et la proximité entre une personne ou un groupe de personnes et les autres. Une densité élevée de processus de protection et régulation des flux se traduit effectivement en une accessibilité moindre de la personne ou des personnes et constitue un haut niveau de *privacy*. Ces processus sont évidemment dynamiques et en constante évolution.

Il existe d'après Altman quatre types de processus par lesquels une personne peut assurer sa vie privée ; des mécanismes verbaux, comme chuchoter pour ne pas être entendu, comportementaux, comme la signification non verbale de renfermement sur soi de l'action de se croiser les bras ; environnementaux, comme les murs sa maison ; et finalement culturels, comme savoir qu'il n'est pas permis d'entrer dans une maison, même si la porte est ouverte, ou de lire les messages de quelqu'un, même si son portable est laissé sans surveillance[77]. À travers ces différents mécanismes de *privacy*, les personnes dévoilent tour à tour certaines informations sur elles-mêmes et en retiennent d'autres en fonction du contexte dans lequel elles se trouvent et des personnes avec qui elles désirent les partager. En effet, il y a une portion des processus qui demande de l'agentivité : une personne *exerce* sa vie privée via les différents processus. Toutefois, il y a parmi les quatre types de processus certains qui sont indépendants des personnes comme les facteurs

[77] Altman, *op. cit.*, p.3

environnementaux. On doit souligner cet élément de la définition d'Altman parce qu'il se révèle important pour une future théorie normative d'une protection de la vie privée, laissant entendre que les processus de vie privée ne dépendent pas exclusivement des personnes, mais également de la structure même de leur environnement. Un second point mérite d'être souligné en ce qui a trait cette définition processuelle : puisque le propre de la vie privée réside à même les mécanismes servant à protéger des éléments quelconques, on comprend pourquoi une intrusion ou une violation d'un de ces mécanismes est suffisante pour parler d'une atteinte à la vie privée. Constater que quelqu'un a voulu forcer la serrure de son appartement engendrera un sentiment d'intrusion, même s'il n'est pas parvenu à entrer dans la propriété, tout comme le fait d'avoir son téléphone sous écoute constitue une atteinte aux processus de *privacy*.

Pour conclure, l'approche processuelle permet à première vue de se réconcilier avec l'ensemble des défis théoriques posés par la notion de vie privée. D'abord, elle offre la possibilité d'un concept de vie privée cohérent et unique : la vie privée est l'ensemble des processus qui servent à réguler l'accès des autres à soi. Cette définition respecte également le critère d'objectivité que nous nous sommes donné plus tôt. Elle n'intègre aucun jugement moral sur ce qui devrait être considéré comme privé. Elle permet en même temps de rendre compte de l'attribut relatif et dynamique de la vie privée, dont les processus peuvent être différents d'une personne et d'une société à l'autre ainsi qu'évoluer dans le temps. Le problème de la vie partagée trouve aussi réponse puisque les processus de *privacy* ne servent pas uniquement à rendre inaccessible l'individu, mais également les choses qui sont considérées privées par une ou plusieurs personnes, comme une discussion ou un moment d'intimité. Une définition processuelle permet enfin de comprendre la violation de vie privée non seulement en matière d'atteinte à ses informations (ou une autre partie de l'individu), mais également, et surtout, en termes de transgression des processus de *privacy*. C'est-à-dire qu'une atteinte aux mécanismes de *privacy* est suffisante pour constituer une atteinte à la vie privée puisque ceux-ci sont constituants de cette dernière. En effet, il n'est pas nécessaire qu'une personne accède à ce qui est tenu comme privé dans la vie d'une autre pour que cette dernière juge qu'elle a été victime d'un tort ; une simple tentative de contournement ou d'atteinte à ces mécanismes de *privacy* est suffisante pour sentir la violation puisque ces mécanismes sont constitutifs de la vie privée.

Une définition de la vie privée

Voici qu'une définition de la vie privée est établie. Ce chapitre a permis de poser les bases théoriques qui serviront au reste de l'analyse. Il est maintenant établi qu'il y a une chose identifiable et singulière qu'on peut appeler "vie privée". Alors que cette chose peut se définir de plusieurs façons, pour les fins de ce mémoire, la vie privée référera à *l'ensemble des processus et stratégies par lesquels les individus essaient de rendre leur personne ou leurs relations intimes inaccessible aux autres*. Cette définition offre une compréhension exempte de considérations normatives sur ce qui devrait ou non demeurer privé. Les conceptions sur ce qui devrait appartenir au domaine de la vie privée diffèrent tellement de société en société, d'époque en époque et même de personne en personne qu'il semble en effet inutile d'essayer de le circonscrire. Par contre, la vie privée effective s'exprime toujours par les moyens mis en place pour protéger ce qui est déterminé comme devant l'être. Ces moyens peuvent prendre plusieurs formes et avoir différents degrés d'efficacité, mais ils sont à la fois la substance et la manifestation de la vie privée. Sans moyens de *privacy*, il n'y a pas de vie privée.

Cette définition implique deux éléments qui seront essentiels pour le reste de notre analyse. D'abord, la vie privée est un ensemble dynamique dépendant partiellement de la personne qui met en place certains des mécanismes, mais également des propriétés et structures de l'environnement physique et social dans lequel se trouve cette personne, soit les processus sociaux et environnementaux d'Altman. Ainsi, il y a une portion des processus de *privacy* accessibles aux personnes qui sont hors de leur contrôle et pour lesquels il appartient tantôt aux institutions gouvernementales, aux architectes ou encore aux programmeurs, par exemple, de les mettre en œuvre afin d'offrir la possibilité aux personnes de maintenir un degré de *privacy* dans certains endroits ou contextes où les autres processus sont insuffisants. Ce dernier constat sur la vie privée sera particulièrement important pour les prochains chapitres. Alors que le deuxième chapitre met en lumière le manque de processus de *privacy* du monde numérique, le troisième pose des arguments éthiques en faveur de la mise en place de tels processus sociaux et environnementaux dans l'environnement numérique, puisque, comme il sera démontré, il s'agit d'un contexte dans lequel les personnes n'ont autrement peu ou pas de moyens de privacy. Ensuite, le deuxième élément mis en valeur par cette définition est le caractère « sensible » des mécanismes de *privacy*. Ces derniers sont tout aussi constitutifs de ce que l'on appelle « vie privée » que les choses qu'ils servent à protéger. C'est pourquoi une atteinte à un processus de privacy, même infructueuse, est

suffisante pour parler de violation de la vie privée. Ces deux caractéristiques de la vie privée permettront de comprendre comment les dynamiques propres au monde numérique affectent particulièrement cette dernière.

Ce premier chapitre a défini la vie privée de façon objective, sans prétention normative. Maintenant que la question du « quoi » est éclaircie, il convient de revenir à la question normative précédemment mise de côté : le « pourquoi la vie privée? » Faut-il vraiment protéger cette dernière et garantir les moyens de *privacy*, et si tel est le cas, pour quelles raisons? Toutefois avant de pouvoir s'y attaquer, il semble essentiel de comprendre, à la lumière de notre définition de la vie privée, le contexte particulier qui met son statut en jeu et qui nous amène à nous poser ces questions, soit le contexte de l'utilisation massive des données par les technologies de l'information. Ce sera l'objet du prochain chapitre.

A child born today will grow up with no conception of privacy at all

Edward Snowden

CHAPITRE 2 : LA VIE PRIVÉE DANS LE CONTEXTE NUMÉRIQUE

En 1993, un dessin de presse par Peter Steiner montre deux chiens derrière un écran d'ordinateur. On peut lire dessous "On the internet, nobody knows you're a dog." Ceci représente bien la croyance populaire de l'époque, soit que l'internet est un lieu d'anonymat où quiconque peut naviguer sans y être démasqué. C'est à ce moment que l'internet, autrefois réservé à des cercles fermés de chercheurs et de scientifiques, commence à être popularisé et rendu accessible au grand public[78]. Le dessin de Peter symbolise l'idéologie alors associée à l'avènement du web : un endroit exempt de toute régulation où les utilisateurs peuvent agir et interagir de façon complètement libre[79]. La possibilité de rester anonyme qu'offre cet espace participe à ce sentiment de liberté. En effet, dans le monde numérique de 1993, les utilisateurs peuvent passer par des sites anonymes, brouillant leur adresse IP, et il est, à cette époque, pratiquement impossible d'identifier qui a fait quoi, où et avec qui sur le web[80]. Toutefois, la possibilité et la sensation d'anonymat ont rapidement disparu avec l'avènement du Web 2.0[81]. Ce dernier, aussi qualifié de « cyber espace, » dépasse largement les limites du simple « internet », ce médium "through which your e-mail is delivered and web pages get published"[82]. Pour Lessig Lawrence, le « *Cyberspace*, » désigne quelque chose de bien plus large et riche qu'internet[83]. Certes, internet participe à cet espace, dont il est en quelque sorte le socle, mais cet espace a largement débordé des pages web. Il est aujourd'hui omniprésent dans le monde, et de plus en plus, les personnes sont en interaction constante avec celui-ci. Il est présent même pendant les rares instants où les gens ne sont pas devant des écrans, via l'armée d'objets connectés qui font rapidement leur place dans le quotidien. Il s'agit d'un espace auquel tous participent que ce soit conscient ou non, mais qui représente littéralement

[78] Lawrence Lessig, *C o d e*, (Basic Book, 2006): 2.
[79] Lessig, *ibid*.
[80] *Ibid*., p.16, p19.
[81] *Ibid*., p.33
[82] *Ibid*., p.9
[83] *Ibid*.

une seconde vie pour une large portion de la population, notamment chez les plus jeunes[84]. Plusieurs y passent des centaines d'heures chaque mois[85]. Or, le design de ce cyber espace a énormément évolué, en même temps que toutes ses nouvelles fonctionnalités. Ce qui était autrefois une toile obscure et anonyme est devenu un outil de traçabilité de l'information. Une simple transaction par carte de crédit peut aujourd'hui être liée à une adresse courriel, puis une adresse IP et à l'ensemble des activités en ligne d'une personne[86]. Ainsi, vingt ans après le dessin de Steiner, on retrouve dans le New Yorker celui de Kaamran Hafeez, en réponse au premier: "Remember when, on the internet, nobody knew who you were." Cette nouvelle illustration montre avec humour comment la perception publique du web en matière d'anonymat et de vie privée a changé en seulement deux décennies.

Ainsi, les avancées technologiques liées à l'amélioration du traitement et du stockage de données, aussi attrayantes soient-elles, sont également source d'inquiétude parce qu'elles menacent la vie privée des personnes. En effet, la numérisation massive, la récolte incessante de données via les objets connectés et les plateformes informatiques, ainsi que le raffinement algorithmique posent des enjeux inédits au maintien et à la protection de la vie privée. Autre fois promesse de liberté et d'accessibilité, la toile qu'ont tissé le web et l'ensemble des objets connectés est devenue un réseau épais dans lequel les comportements sont épiés et enregistrés, une toile sur laquelle il est désormais impossible de demeurer anonyme.

Alors que le concept de vie privée est présent dans la littérature depuis des décennies, ces enjeux spécifiques aux technologies numériques sont relativement nouveaux. Cette nouvelle réalité, et les enjeux qu'elle soulève ont d'ailleurs donné lieu à de nouveaux courants théoriques dans plusieurs domaines, dont la philosophie. L'éthique des données s'intéresse par exemple aux problèmes moraux liés aux données numériques. L'éthique des algorithmes traite quant à elle des questions soulevées par la complexité croissante des algorithmes. Si ces branches d'étude sont encore jeunes et en développement, elles offrent déjà plusieurs bases théoriques et outils analytiques pour interpréter les enjeux en question, dont ceux liés à notre objet d'étude : la vie privée. Ainsi, afin de comprendre la nature des enjeux auxquels cette dernière est aujourd'hui

[84] danah boyd et Alice Marwick, « Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies », *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, septembre 2011, 1-29, https://doi.org/10.31219/osf.io/2gec4.
[85] Lessig, *op. cit*., p.9.
[86] Bernard E. Harcourt, *Exposed*, éd. par Harvard University Press, 2015 : 159.

confrontée ce chapitre présente les grands éléments participant à la détérioration de la vie privée à l'aide des théories développées pas les philosophes de l'éthique des données. Cela permettra notamment de mettre en relation les technologies de l'information avec notre concept de vie privée, mettant en lumière les menaces spécifiques qui se posent et définissant les concepts nécessaires pour comprendre tout argument en faveur d'une « vie privée numérique. »

Selon la philosophe Carissa Véliz, au moins trois éléments jouent un rôle dans la dégradation de notre vie privée numérique : d'abord l'utilisation massive des données, ensuite la culture de surveillance et enfin la croyance erronée que la vie privée est une valeur dépassée.[87] Le présent chapitre reprend et développe les deux premiers éléments identifiés par Véliz pour comprendre comment la structure numérique s'est construite de façon antagoniste à tout principe de *privacy* et pour décortiquer les mécanismes qui contreviennent au maintien d'une vie privée en ligne. Le troisième enjeu identifié par Véliz concernant la valeur supposément obsolète de la vie privée fera quant à elle l'objet du troisième chapitre.

La première section du présent chapitre traite des données, objet de convoitise au centre du tumulte numérique. Cette section reprend les bases théoriques développées par les éthiciens des données afin de démontrer en quoi l'utilisation de ces dernières pose un enjeu inédit à la vie privée. Afin de bien rendre compte du problème, on doit d'abord se pencher sur la nature même de ces données et sur leur fonction, mais également comprendre les dynamiques de pouvoir à la source de leur utilisation massive. C'est pourquoi ce chapitre emprunte également à la sociologie alors que la deuxième section s'intéresse aux structures qui maintiennent des dynamiques de partage incessant de l'information. Afin de donner du contexte à ces dynamiques, certains éléments historiques sont également intégrés dans ce chapitre. L'objectif final est de présenter le contexte numérique particulier dans lequel les nouveaux enjeux de vie privée reposent. Ce faisant, on entend démontrer comment la structure même de l'environnement numérique tel qu'il s'est développé n'est pas propice ni au développement ni au maintien de stratégies de vie privée.

LES DONNÉES : OBJET DU PRIVÉ

On ne peut parler d'enjeux de vie privée dans le contexte numérique sans parler des données. Les données sont l'objet de convoitise à la source de l'assaut mené contre la vie privée.

[87] Carissa Véliz, « Privacy is Power », éd. par Kindle Edition, 2021: 31-32.

Véliz identifie la source de cette course à l'or numérique (les données) à leur transformation en une ressource à valeur monétaire. À l'aurore de l'internet, au moment où de nombreuses startups essayaient de percer un marché jusqu'alors exempt d'un modèle d'affaire rentable, une toute petite compagnie du nom de Google change la donne du tout au tout. Le moteur de recherche commence alors à utiliser les données de ses utilisateurs pour vendre des publicités.[88] C'est précisément ce changement dans le modèle d'affaire de la compagnie - aujourd'hui la deuxième plus profitable au monde après Apple[89] - qui a complètement changé le paradigme numérique : les utilisateurs du web sont devenus le produit plutôt que d'être le client. Voici, simplement résumé, ce qui a transformé un outil de démocratisation de l'information en une usine à données personnelles et qui a inauguré « l'âge de la surveillance numérique. »[90] Mais avant de creuser les enjeux liés à l'utilisation des données, et pour comprendre cette transformation, il faut d'abord revenir à la base de ce qu'est une donnée.

Qu'est-ce qu'une donnée?

Selon le professeur Serge Abiteboul, une donnée est « une description élémentaire d'une réalité »[91]. Ce peut être une observation ou une mesure. Il s'agit d'un « élément brut qui n'a pas encore été interprété ni mis en contexte »[92]. En interprétant une donnée ou en la corrélant à d'autres données et en faisant du sens des liens entre celles-ci, l'information comprise dans la donnée peut générer du savoir ou de la connaissance. Ainsi une donnée, considérée isolément, est peu utile. Par exemple « 19 » est une donnée. Sans contexte, cette donnée est inintéressante. Par contre, si savoir que « 19 » est le nombre de fois qu'une personne a regardé son téléphone en une heure donnée est une information intéressante. Ce qui est encore plus intéressant est d'enregistrer ces données (le nombre de fois qu'X regarde son téléphone) à chaque heure pendant une année de les corréler avec d'autres types de données : le jour de la semaine, le moment de la journée, la géolocalisation de

[88] Véliz, *op. cit*, p. 34.
[89] Marty Swant, « The 2020 World's Most Valuable Brands », *Forbes Media*, juillet 2020, https://www.forbes.com/the-worlds-most-valuable-brands/#579b01b4119c.
[90] Véliz, *op. cit.*, p. 34.
[91] Adrien Basdevant et Jean-Pierre Mignard, *L'empire des données: essai sur la société, les algorithmes et la loi* (Don Quichotte éditions, 2018): p. 10., citant Serge Abiteboul, « Sciences de données. De la logique du premier ordre à la Toile », leçon inaugurale à la chaire Informatique et sciences numériques du Collège de France prononcées le jeudi 8 mars 2012.
[92] Maya Bacach-Beauvallet et al., « Le rôle des données et des algorithmes dans l'accès aux contenus », Premier rapport de la série Les mutations de la mise à disposition de contenus audiovisuels à l'ère du numérique : conséquences et enjeux (CSA Lab, 2017): p.7.

X, etc. En agrégeant une multitude de données, il est donc possible de tirer des informations intéressantes. C'est cette possibilité de manipulation des données pour en tirer des connaissances qui les rendent si attrayantes : en effet, « [les] données « tirent leur force » et leur valeur des opérations de production, circulation, agrégation et mise en forme dont elles font l'objet »[93].

La production d'information via l'analyse de données n'est pas un phénomène nouveau. Le monde transpire de données; de la température de l'air ambiant, à la couleur du ciel, jusqu'à l'émission de radio qui joue au moment où ces lignes sont lues. Ces données sont constamment enregistrées et analysées par les personnes afin de naviguer dans leur environnement. Si les cerveaux humains sont d'excellents capteurs de données, leur capacité à les stocker et à les analyser est toutefois limitée. Celle des ordinateurs, en revanche, est nettement supérieure[94]. Ainsi la numérisation des données offre des possibilités d'analyse, et donc de production d'information nettement supérieure à celle des humains. Les données sous leur forme numériques peuvent alors prendre plusieurs formes : texte, image, enregistrement audio, etc.

Louis Sagnièrese explique en quoi le traitement numérique de données offre des possibilités aussi avantageuses. Il identifie trois éléments qui expliquent la différence entre le traitement de l'information dans le monde naturel et celui dans le monde numérique. D'abord, manipulation et la valorisation de l'information sont facilitées parce que cette dernière est devenue *tangible* dans le monde informatique[95]. En effet, l'information, au lieu de se dissiper au moment de sa production, ou d'être oubliée par le cerveau humain, est enregistrée sur un support numérique. Une fois numérisée, l'information peut être manipulée, catégorisée et recherchée. Du fait qu'elle soit enregistrée découle ensuite un second élément : l'information devient *pérenne.* C'est-à-dire que l'information peut être conservée indéfiniment, à moins d'être effacée[96], et peut être accumulée, permettant une analyse des données et de leur évolution dans le temps. Enfin, la troisième caractéristique des informations numériques identifiée par Sagnièrese est leur parfaite *reproductibilité*[97]. On peut créer une infinité de copies identiques d'une information numérique. Cette propriété permet un partage facilité de l'information, mais également une utilisation simultanée de cette dernière par de multiples utilisateurs. Bref, les ordinateurs permettent de

[93] *Ibid*.
[94] Lessig, *op. cit*., p.292.
[95] Sagnières, *op. cit*., p.73.
[96] *Ibid.*
[97] *Ibid.*

quantifier, mesurer, comparer et conserver l'information, offrant une emprise sans précédent sur celle-ci en plus d'un accès à de la méta information, soit de l'information sur l'information.

Voici donc le premier constat sur le changement de paradigme qu'a engendré la numérisation du monde : les données, dans leur forme numérisée, permettent une manipulation et un traitement de l'information surhumain. Notons tout de suite que pour les fins de ce travail, le terme « donnée » référera désormais exclusivement aux données numériques. Maintenant, qu'est-ce qui, exactement, fait de l'accès aux données en enjeu de vie privée ? Les possibilités qu'offre le traitement augmenté des données motivent une tendance à capter, enregistrer et cumuler toujours plus de données. Or les données concernant les personnes et leurs activités ne sont pas épargnées, au contraire. Dans un monde centré sur l'humain, les données dites « personnelles » sont rapidement devenues une denrée recherchée alors qu'un éventail croissant de technologies vise à capter divers aspects de la vie humaine et à les traduire en ensembles de données numériques « afin de pouvoir 'capitaliser' sur les risques et opportunités dont nous sommes porteurs »[98]. Ceci pose des enjeux inédits pour la vie privée.

Les données : un enjeu pour la vie privée

« You are your information »[99]. C'est du moins la thèse défendue par Luciano Floridi, théoricien de la philosophie de l'information et de l'éthique informatique. Floridi propose une interprétation qu'il qualifie lui-même de radicale : "one that takes into account the informational nature of ourselves, and our interactions as inforgs"[100]. L'auteur s'oppose notamment à une conception faisant de l'information personnelle un objet de propriété. Selon cette dernière approche, l'information personnelle serait la propriété des personnes au même titre que leurs biens matériels[101]. Une telle interprétation contribue selon lui à une culture marchande régie par des

[98] Antoinette Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », *Le numérique et les droits et libertés fondamentaux, Étude annuelle du Conseil d'État* (Paris, 2014).
[99] Floridi, « The ontological interpretation of informational privacy », *op. cit*., p. 195.
[100] David Bawden et Lyn Robinson, « "The dearest of our possessions": Applying Floridi's information privacy concept in models of information behavior and information literacy », *Journal of the Association for Information Science and Technology* 71, nº 9 (2020): 1032, https://doi.org/10.1002/asi.24367, citant Luciano Floridi, *The fourth revolution: how the infosphere is reshaping human reality* (Oxford University Press, 2014).
[101] Michael Nycyk, « From data serfdom to data ownership: An alternative futures view of personal data as property rights », *Journal of Futures Studies* 24, nº 4 (2020): 25-34, https://doi.org/10.6531/JFS.202006_24(4).0003.

rapports d'échanges et dans laquelle l'information pourrait alors faire l'objet de transaction comme le reste des possessions[102]. Selon lui, si les données personnelles « appartiennent » aux personnes, elles leur appartiennent de la même façon que leur main et leur corps sont « à » elles.[103] L'argument principal présenté par Floridi pour appuyer sa thèse est que l'information personnelle est une partie constitutive de l'identité et de l'individualité d'une personne, de ce qu'une personne est et ce qu'elle peut devenir[104].

Les personnes, à plusieurs égards, sont des entités informationnelles. Socialement, on ne « connaît » l'autre qu'à travers l'image que l'on s'en est construite et que l'on continue de se construire à chaque interaction. C'est un processus intellectuel qui requiert des informations entrantes; les formes de son visage, le son de sa voix, ses attitudes et traits de personnalité. La somme de ces informations, toujours partagée de façon partielle à autrui, forme d'une certaine façon l'identité d'une personne. Ainsi, Floridi conçoit chaque personne comme étant constituée de ses informations, faisant de la '*informational privacy*' un type de vie privée à part entière qui est selon lui central[105].

C'est pour cette raison que Floridi maintient qu'il faut considérer une violation de l'information personnelle non pas comme un vol, mais plutôt comme un « enlèvement numérique » (*digital kidnapping*)[106]. Contrairement à l'enlèvement classique, les données personnelles ne sont physiquement enlevées, mais plutôt clonées, ou dupliquées, mais il n'en demeure pas moins que ces informations constituent, au moins en partie, la personne ayant subi l'intrusion. Il s'agit d'une agression à l'encontre de l'identité personnelle. Cette approche permet de changer la perspective concernant la protection des données personnelles, appuyant par exemple l'idée que le vol d'identité, un crime en forte croissance, dépasse largement le simple vol de données. Un vol d'identité confère en quelque sorte au pirate une identité « augmentée »[107], ou

[102] Floridi, « The ontological interpretation of informational privacy », *op. cit*., p. 194
[103] Luciano Floridi, « Four challenges for a theory of informational privacy », *Ethics and Information Technology* 8, nº 3 (2006): p.8, https://doi.org/10.1007/s10676-006-9121-3.
[104] Floridi, « Four challenges for a theory of informational privacy », p.8-9.
[105] Bawden et al., *op. cit.,* p.1034.
[106] Floridi, « The ontological interpretation of informational privacy », *op. cit.,* p.195.
[107] *Ibid.,* p.196.

bonifiée et laisse, en revanche, la victime avec des conséquences non seulement financières, mais également physiques et psychologiques comme le démontrent de plus en d'études[108]. Pour Floridi :

> Looking at the nature of a person as being constituted by that person's information allows one to understand the right to informational privacy as a right to personal immunity from unknown, undesired or unintentional changes in one's own identity as an informational entity, either actively – collecting, storing, reproducing, manipulating, etc. one's information amounts now to stages in stealing, cloning or breeding someone else's personal identity – or passively – as breaching one's informational privacy may now consist in forcing someone to acquire unwanted data, thus altering her or his nature as an informational entity without consent. Brainwashing is as much a privacy breach as mind-reading.[109]

En en adoptant l'approche de Floridi, il apparaît dès lors évident que les données confèrent un accès réel et immédiat aux personnes. C'est pourquoi l'accès aux données personnelles peut et doit être considéré comme une menace sérieuse dans une perspective de régulation de l'accès à soi qui a été établie comme la définition de la vie privée. Or, il existe de grands incitatifs à faire la collecte de ces données alors que l'on assiste à la mise en données de nos sociétés sous l'ère des « données massives » (*Big data*)[110].

La collecte des données à l'ère des « données massives »

Plusieurs facteurs participent au phénomène du *Big data*. Les activités humaines se déplacent de plus en plus vers le monde numérique. La plupart des sphères d'activités dépendent aujourd'hui en tout ou en partie des technologies[111]. Ainsi les personnes produisent de plus en plus de '*digital footprints*' (traces digitales), tellement, que l'on réfère à ces données générées par les différentes activités humaines par le terme « *Big data.* »[112] Ces données sont générées de multiple façon :

> This is not only data explicitly entered by the user, but also numerous statistics on user behavior: sites visited, links clicked, search terms entered, etc. (…) Big data does not only

[108] Katelyn Golladay et Kristy Holtfreter, « The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes », *Victims and Offenders* 12, nº 5 (3 septembre 2017): 741-60, https://doi.org/10.1080/15564886.2016.1177766.
[109] Floridi, « Four challenges for a theory of informational privacy », *op. cit*., p.7.
[110] Bacach-Beauvallet et al., *op. cit*., p.7.
[111] Pierre Beckouche, « La révolution numérique est-elle un tournant anthropologique ? », Le Débat, 193, nº 1 (2017): 153-66.
[112] Terence Craig, Mary E. Ludloff, et Jennifer Geetter, *Privacy and big data*, *Computer* (O'Reilly Media, 2011), https://doi.org/10.1109/MC.2014.161.

> emerge from Internet transactions. Similarly, data may be collected when shopping, when being recorded by surveillance cameras in public or private spaces, or when using smartcard-based public transport payment systems.[113]

Or, toutes ces données que génèrent les personnes par leurs activités quotidiennes sont l'objet de convoitise de multiples organisations en raison de leur potentielle profitabilité[114]. Ainsi, le phénomène du Big data n'est pas seulement le fait d'une activité numérique accrue dans les sociétés, mais également, et surtout, d'une culture grandissante de collecte agressive des données. Certains parlent même d'un « abus de la collecte excessive de données »[115]. Cet excès est bien illustré par la populaire technique du '*third-party tracking*' (suivis tiers) : « a practice which allows a tracker to harvest extensive amounts of personal user data from a variety of first-party sources in the online environment and across different devices such as smartphones, tablets and laptops/computers, ultimately building a comprehensive user profile. »[116] Les champions du suivi tiers sont Alphabet, Google, Microsoft et Facebook[117]. Les fameux '*cookies*', ces petits capteurs d'information, permettent notamment à ces compagnies d'enregistrer les données produites sur d'autres plateformes que les leurs. C'est pourquoi des entreprises comme Facebook admettent avoir des données sur des personnes même si celles-ci n'ont jamais eu de compte sur leur réseau social[118]. Pour assouvir cette soif de données, les moyens de collectes se donc multipliés, les entreprises passant d'une collecte passive à une quête proactive de cumuler toujours plus de données. On pense également à la prolifération des objets connectés qui contribuent également à ce que chaque personne « produise » quotidiennement de plus en en plus de données, lesquelles sont constamment collectées par de multiples entités, souvent à leur insu de ces personnes. Aujourd'hui, sans même que l'utilisatieur ait cliqué sur un lien publicitaire, les traqueurs ont déjà

[113] Jeroen van den Hoven, Martijn Warnier, et Pieters Wolter, « Privacy and Information Technology », in *The Stanford Encyclopedia of Philosophy*, Summer 2020 Edition, s. d., https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.
[114] Viktoria H.S.E. Robertson, « 'Excessive data collection: Privacy considerations and abuse of dominance in the era of big data », Common Market Law Review, nº Issue 1 (2020): 161-90.
[115] *Ibid*.
[116] *Ibid*, p.2.
[117] *Ibid*.
[118] David Ingram, « Facebook fuels broad privacy debate by tracking non-users », Reuters [ONLINE] , 2018, https://www.reuters.com/article/us-facebook-privacy-tracking-idUSKBN1HM0DR.

probablement analysé le temps d'attention exact consacré à une annonce, et repéré les mouvements oculaires de même qu'identifié les émotions suscitées chez l'utilisateur via sa propre caméra[119].

Véliz relate qu'en 2003 après avoir constaté la profitabilité de son nouveau modèle d'affaires, Google est rapidement passé de la simple récupération des données produites par les utilisateurs interagissant avec son site web et de leur utilisation pour améliorer son service, à la chasse aux données des utilisateurs dans le but manifeste de publicité ciblée, comme le démontre entre autres l'un des brevets déposés par la compagnie cette année-là[120]. Il est par ailleurs estimé que le géant du détail Walmart collecte à lui seul plus de 2.5 pétaoctets de données chaque heure à partir des transactions de ses clients[121]. En ce qui concerne la quantité d'information, cela représente environ l'équivalent de l'ensemble des documents contenus dans toutes les librairies de recherche universitaire américaines combinées[122]. Google et Walmart sont loin d'être les seules compagnies à faire de la collecte de données. De nos jours, l'économie digitale est plus importante que jamais et des compagnies de toutes tailles se prêtent à la course aux données. Il y a une réelle culture de la collecte des données incarnée dans le *Big Data*. On pratique la collecte de façon frénétique. On collecte sans but précis des données dont l'utilité potentielle est encore incertaine, simplement par ce qu'on le peut :

> Les *big data*, au contraire de la minimisation, c'est la collecte maximale, automatique, par défaut, et la conservation illimitée de tout ce qui existe sous une forme numérique, sans qu'il y ait, nécessairement, de finalité établie a priori : l'utilité des données ne se manifeste qu'en cours de route, à la faveur des pratiques statistiques de *data-mining*, de *machine learning*, etc., des données a priori inutiles peuvent se révéler extrêmement utiles à terme à des fins de profilage par exemple, et gagnent en utilité au fur et à mesure que grossissent les jeux de données.[123]

---

[119] Loin d'être de l'ordre de la fiction, ces technologies sont présentées dans deux brevets déposés par Facebook; "Techniques for Emotion Detection and Content Delivery" en 2015 et "Dynamic Eye Tracking Calibration" en 2017. Les deux brevets proposent des technologies permettant d'analyser les personnes à travers la caméra en temps réel pendant qu'elles naviguent en ligne. Voir Susanna Paasonen, « Affect, data, manipulation and price in social media », *Distinktion* 19, nº 2 (2018): 214-29, https://doi.org/10.1080/1600910X.2018.1475289.

[120] Véliz, *op. cit.*, p. 36.

[121] Harcourt, *op. cit.,* p.136

[122] Rodney Brown, « Defition : Petabyt », TechTarget, s. d., https://searchstorage.techtarget.com/definition/petabyte.

[123] Antoinette Rouvroy, « Homo juridicus est-il soluble dans les données? », *Law, Norm and Freedoms in Cyberspace/ Droit, norms et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, 2018, p.427.

On trouve ainsi un nombre grandissant d'outils et de techniques, de plus en plus efficaces, qui permettent de collecter les données en abondance. Les capacités de stockage de ces données ayant également augmenté, l'univers digital grossit de façon exponentielle chaque année[124]. La quantité de données dans le monde numérique est simplement exorbitante : "eveything we do leaves a digital footprint, so much that we had to give it a name : big data"[125]. Or les activités des utilisateurs composent 70% de cette masse de données[126]. Ce sont les comportements des individus sur le web, traduits en un essaim de données qui compose ce fameux *Big data*. Bref, la quantité et l'éventail de données produites aujourd'hui permettent d'obtenir de l'information de plus en plus raffinée et précise sur les personnes. Toutes ces données, pièces d'information sur les comportements, les désirs, préférences, complexes et humeurs des personnes sont plus qu'une fenêtre ouverte sur ces dernières, ce sont des fragments des personnes elles-mêmes qui sont collectées et manipulées. La prochaine section explique comment le traitement de ces innombrables données pose des enjeux pour la vie privée outre l'argument de Floridi.

Dans les prochaines sections, nous démontrons comment le traitement algorithmique de ces données massives présente des enjeux additionnels pour la vie privée. Grâce aux algorithmes, les données offrent non seulement un accès direct aux personnes, comme démontré plus tôt avec les thèses de Floridi, mais également une fenêtre sur les comportements futurs des personnes en raison du potentiel prédictif des données.

Les techniques algorithmiques de traitement des données

Si les données sont une porte ouverte sur l'identité, la personnalité ou encore l'intimité des personnes au moment de leur collecte, elles offrent également un potentiel prédictif impressionnant. C'est-à-dire qu'elles peuvent fournir des informations sur les comportements futurs des personnes. Ceci s'explique par la capacité nouvelle d'analyse de l'information qu'offrent les nouvelles techniques algorithmiques. Comme mentionné plus tôt, les nouvelles techniques de traitement de l'information offrent une capacité inégalée de traitement de larges quantités de données, traitement qui offre à son tour un accès à de l'information autrement inaccessible. La logique humaine étant dépassée par le volume initial d'information à analyser, les

[124] Craig et al., *op. cit*., p.4.
[125] *Ibid*.
[126] *Ibid*.

formules informatiques (algorithmes) permettent d'analyser une quantité nettement supérieure de données, à la fois plus rapidement et avec plus d'exactitude que les humains[127].

Lorsque l'on parle « d'intelligence artificielle », on réfère généralement aux différentes techniques de traitement d'information, soit aux algorithmes. Ces derniers occupent une place cruciale au sein des récentes innovations dans le domaine des technologies de l'information. Ils sont la substance de tout programme informatique, y compris les programmes d'IA. Plus précisément, un algorithme est une « suite finie d'étapes ou d'instructions produisant un résultat à partir d'éléments fournis en entrée. Une recette de cuisine est, par exemple, un algorithme, de même que les règles de fonctionnement d'un moteur de recherche sur Internet »[128], seulement la complexité de la suite utilisée diffère. L'IA met en œuvre une forme excessivement complexe d'algorithmes[129]. Les techniques les plus poussées d'IA sont rassemblées sous la catégorie « d'apprentissage automatique » (*machine learning*), comme l'apprentissage par renforcement (*reinforcment learning*) et l'apprentissage profond (*deep learning*)[130]. Pour remplir leur potentiel analytique, ces dernières nécessitent, en plus d'une énorme puissance de calcul, une quantité faramineuse de données[131]. Les données sont en quelque sort l'essence des moteurs que sont les systèmes de traitement de l'information, et ces moteurs consomment énormément.

La particularité de ces algorithmes est qu'ils permettent non seulement de tisser des liens entre les données de sorte à en tirer de l'information, mais qu'ils ont aussi la propriété « d'apprendre » par eux-mêmes[132]. C'est-à-dire qu'ils deviennent de plus en plus performants à réaliser les tâches auxquelles ils ont été programmés à force de les accomplir. Par exemple, un algorithme de reconnaissance programmé à identifier les images de chats deviendra meilleur à mesure des images qu'il traitera. Ainsi plus grand sera le nombre de données (d'images dans ce cas) avec lesquels l'algorithme est entraîné, meilleur sera sa performance sur de nouvelles données.

---

[127] *Ibid,* p.5.
[128] Conseil constitutionnel, 12 juin 2018, Décision n° 2018-765 (France) référant au Rapport n°350 (Sénat) de Mme Sophie Joissains, fait au nom de la commission des lois, deposé le 14 mars 2018, p. 106-107. (https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm)
[129] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Mifflin Harcourt, 2018): p. 111, https://doi.org/10.1007/s11366-020-09674-8.
[130] Office québécois de la langue française (OQLF), « apprentissage automatique », in *Grand dictionnaire terminologique*, en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061.
[131] Basdevant et Mignard, *op. cit*.
[132] Office québécois de la langue française (OQLF), « apprentissage automatique », in *Grand dictionnaire terminologique*, en ligne : http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061.

La performance d'un algorithme est calculée sur sa marge d'erreur. Ainsi dans le cas de notre algorithme amateur de félin, la marge d'erreur sera équivalente au pourcentage d'images que l'algorithme aura mal identifié. À noter que la performance de l'algorithme dépend du nombre de données, mais également de la qualité du jeu de données sur lequel il est entraîné[133]. En effet, si un algorithme est entraîné à reconnaître des images de chats, mais que toutes les images de chat qui lui ont été présentées sont des chats de couleur blanche, alors il est fort probable qu'il sera peu performant pour reconnaître des chats de couleur noire. En effet, s'il y a des biais présents à même le jeu de données, ces derniers seront reconduits par l'algorithme.

Outre l'identification d'image de chat, certaines techniques algorithmiques permettent par exemple d'identifier des tendances à partir d'événements passés et ainsi de faire des prédictions sur des événements futurs[134]. Les algorithmes prédictifs sont par exemple à la source des recommandations de produits sur les diverses plateformes en ligne. Ils analysent des données provenant de sources diverses, comme les recherches passées des utilisateurs, pour ensuite produire des résultats de recherche personnalisés, en fonction leurs intérêts présumés[135]. Cette capacité « prédictive » peut s'avérer particulièrement problématique lorsque combinée à des pratiques de collecte massive de données et elle pose au moins deux problèmes pour la vie privée.

Le potentiel prédictif des données : d'autres enjeux pour la vie privée

Un premier problème réside dans la véracité des prédictions algorithmiques. Comme exposé plus tôt, les données disponibles, la capacité de calcul augmentée, et le raffinement des algorithmes donnent lieu à des algorithmes de plus en plus performants, et donc à des prédictions de plus en plus exactes lorsque les jeux de données sont adéquats. Or lorsque l'accumulation de données anodines mène à la prédiction d'informations beaucoup plus sensibles, un réel enjeu de vie privée se pose.

L'ensemble des pratiques visant à découvrir les tendances cachées et prédire les tendances futures via la collecte et l'analyse prédictive des données réside dans ce qui est appelé le

[133] Mashael A L Johani, « Personal Information Disclosure and Privacy in Social Networking Sites » (Auckland University of Technology, 2016): p.51.
[134] Akos Rona-Tas, « Predicting the Future: Art and Algorithms », *Socio-Economic Review* 18, nº 3 (2020): 893-911, https://doi.org/10.1093/ser/mwaa040.
[135] Office québécois de la langue française (OQLF), « algorithme prédictif », in *Grand dictionnaire terminologique*, s. d., http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26543863.

'*datamining'*. Un exemple frappant des conséquences du datamining est celui de la compagnie Target qui en 2012 a « appris » qu'une jeune fille de 16 ans était enceinte avant ses propres parents[136]. La compagnie utilisait des algorithmes analysant les habitudes d'achat de leur clientèle afin de cibler des groupes sociaux comme les femmes enceintes pour des fins publicitaires. La jeune fille ayant ainsi commencé à recevoir d'incessantes publicités à saveur de maternité – couches pour bébé, poussettes et vêtements de grossesses, ses parents ont éventuellement contacté Target, implorant la compagnie de cesser d'envoyer ces publicités suggestives à leur adolescente. Et bien, il s'est par la suite avéré que leur fille était effectivement enceinte et que l'algorithme du distributeur géant ne s'était finalement pas trompé[137].

Ce qui est particulièrement frappant dans cette histoire est que l'entreprise n'a eu aucune indication directe sur la maternité de la jeune femme comme l'achat d'un test de grossesse par exemple. Leur prédiction s'est plutôt basée sur l'analyse prédictive des données de consommation. Leur algorithme avait identifié certains changements dans les habitudes consommation, comme l'achat soudain de crème sans parfum ou de certaines vitamines et compléments. On peut supposer que cette prédiction s'est fondée sur l'analyse des données de milliers d'autres clientes qui avaient démontré des changements similaires dans leur consommation et qui ont par la suite acheté poussettes et biberons. Ces informations de consommation, prises isolément, sont sans intérêt. Par contre, associées au compte client de cette jeune femme, elles ont permis qu'un algorithme la classe dans la catégorie de clientes « possiblement enceintes », information que cette cliente n'a pas partagée à Target volontairement. En outre, dans ce cas, la vie privée de la jeune femme a été doublement atteinte lorsque cette information confidentielle a ensuite été révélée à ses parents, conséquence de la puissance prédictive qu'offre l'exploitation des données.

Ceci montre qu'une donnée en apparence innocente et sans intérêt peut, combinée à d'autres données tout aussi anodines, révéler des informations beaucoup plus personnelles sur une personne, et ce par simple inférence. Il nous faut ici souligner ce qu'implique cette dernière conclusion : il n'y a pas seulement les données personnelles qui posent un danger à la vie privée numérique. Une donnée dite « personnelle » est définie comme « toute information se rapportant

[136] Dominique Froment, « Votre épicier en sait peut-être plus sur vous que votre conjoint », *Les Affaires*, s. d., https://www.lesaffaires.com/dossier/creer-l-avenir-maintenant/votre-epicier-en-sait-peut-etre-plus-sur-vous-que-votre-conjoint/541930.
[137] *Ibid*.

à une personne physique identifiée ou identifiable »[138]. Les données personnelles incluent toutes celles qui permettent d'identifier directement une personne, comme le nom, le numéro de téléphone, une adresse postale, un numéro de sécurité sociale ou encore une donnée biométrique de la personne comme sa voix, son empreinte digitale ou son image. Ces données sont généralement déjà protégées par des mesures comme la *Loi sur la protection des renseignements personnels*[139]*,* ou plus récemment par le Règlement Général sur la Protection des Données (RGPD)[140], parce qu'elles constituent en elles-mêmes des informations directement liées à l'identité d'une personne comme un nom ou une adresse par exemple ce qui leur confère une plus grande sensibilité. D'un point de vue de protection de la vie privée, on peut se réjouir de ces mesures relatives aux données personnelles. Toutefois, ce qu'illustre l'histoire de Target est que les nouvelles capacités de manipulation des informations permettent de déceler des tendances de plus en plus subtiles et même de faire des prédictions de plus en plus adéquates à partir du croisement d'ensemble de données sans faire appel aux données personnelles. En somme, les données collectivement générées aujourd'hui ouvrent une fenêtre sur nos comportements individuels de demain :

> Toute donnée numérique, transpirante de nos comportements, aussi peu dense en information lorsqu'elle est considérée isolément, peut aussi nous relier statistiquement à des « profils » ou modèles comportementaux impersonnels, mais tenus pour prédictifs si elle est croisée avec des données émanant d'autres sources et qui peuvent être aussi peu « personnelles », mais en quantité suffisante.[141]

Ces « profils », comme le décrit Antoinette Rouvroy, sont des modèles comportementaux identifiés statistiquement par les algorithmes, comme le profil « possiblement enceinte ». Ceci nous amène au second problème que pose la prédiction algorithmique; soit qu'il n'est en fait pas nécessaire que les prédictions se révèlent juste pour avoir des effets dévastateurs. D'après Rouvroy, alors que la rationalité moderne permettait de trouver des relations causales explicatives entre des phénomènes à partir d'éléments visiblement analogues[142], cette nouvelle rationalité algorithmique est fondée sur l'analyse d'éléments innombrables et a priori sans lien, mais permet

---

[138] Craig et al., *op. cit*.
[139] La Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21), est la loi Canadienne concernant la protection des données. Pour la consulter : https://laws-lois.justice.gc.ca/fra/lois/p-21/
[140]Réglement Générale sur la protection des données (GDPR), Journal officiel de l'Union européenne, 27 Avril 2016.
[141] Rouvroy, « Homo juridicus est-il soluble dans les données? », *op. cit.,* p.425.
[142] Par « visiblement » on entend qui pourraient être identifié par observation.

d'en tirer des corrélations statistiquement significatives et qui seraient autrement presque impossibles à identifier : « [devient] alors actuel par avance ce qui n'existait que sur le mode de la potentialité »[143]. En d'autres termes, les algorithmes dévoilent non seulement des corrélations cachées, mais également des tendances permettant de construire des profils, qui à leur tour permettent d'effectuer des prédictions. Une fois posées, ces prédictions qui n'existaient jusqu'alors qu'en puissance, deviennent dès lors effectives puisqu'exploitables – et exploitées. Constater la probabilité statistique jusqu'alors insoupçonnée influence l'opinion et le comportement des personnes qui agissent en conséquence de sorte que ce qui n'était que probable devient réalité.

Les stratégies de marketing propulsées par ces algorithmes de prédiction sont un exemple parmi tant d'autres du phénomène de prophétie autoréalisatrice que provoque le régime de vérité numérique. Mais l'enjeu entourant la confidentialité des données dépasse largement la manière dont on nous fait de la publicité. Il s'agit d'un débat sur la collecte et l'utilisation de nos informations personnelles d'un point de vue commercial et politique puisque ces données ouvrent la porte à des pratiques de plus en plus intrusives de surveillance des comportements et d'influence de ces derniers[144]. En somme, le manque de vie privée numérique conduit à des pratiques hautement intrusives qui à leur tour suscitent une conformité au modèle de la part des agents qui perdent une forme d'autonomie. » Comme le formule Rona Tas : "[the] danger of algorithmic anticipation of individual actions is that it can seriously limit human agency and can pre-emptively colonize the future"[145]. Les données peuvent fournir beaucoup d'information sur le monde, mais elles ne sont jamais un portrait exact de la réalité, seulement une représentation particulière de ce dernier. De même, les prédictions faites à partir de l'analyse de tendances sont toujours le résultat de liens tissés entre des phénomènes du passé ayant causé les résultats d'un passé plus récent, et donc n'intégrant jamais au modèle la possibilité qu'une nouvelle variable alors inconnue change la donne pour le futur[146]. Ce lien étroit entre la vie privée et l'autonomie sera repris dans le troisième chapitre.

Voici donc ce qui conclut la description des effets pervers de la collecte des données sur la vie privée. Les données cristallisent l'information sur les personnes, facilitant d'une part l'accès

[143] Rouvroy, « Homo juridicus est-il soluble dans les données? », *op. cit.*
[144] Craig et al., *op. cit*.
[145] Rona-Tas, op. cit., p.2.
[146] Cathy O'Neil, *Weapons of Math Destruction: how big data increases inequality and threatens democracy*, Kindle Edi, 2016: p. 204.

direct à ces dernières, mais également l'accès futur en permettant d'autre part la production de prédiction sur celles-ci. On tire au moins trois conclusions au sujet des données. D'abord, il y a aujourd'hui une économie des données des utilisateurs puisqu'elle une source de revenus pour les entreprises qui les collectent, les minent, les revendent ou les conservent simplement pour usage ultérieur – ne sait-on jamais. Ensuite, il n'y a pas seulement les données dites « personnelles » qui peuvent être l'objet d'une intrusion dans la vie privée. Toutes les données sont sensibles à un certain degré, parce qu'elles ont le potentiel de révéler des informations personnelles via le *datamining*, même si elles n'en fournissent pas *a priori*. Enfin, les données récoltées sur les individus sont le carburant pour des techniques d'IA dont les prédictions ont des conséquences directes sur les personnes, permettant notamment de tirer profit de ces mêmes personnes. En somme, la migration de l'information vers le numérique, combinée à la monétisation des données, ont fait du privé un marché. La prochaine section s'intéresse à la structure du cyber espace et les dynamiques en place qui exacerbent les effets négatifs de l'utilisation massive des données sur la vie privée.

LA STRUCTURE DU CYBER ESPACE : DES ARCHITECTURES DE POUVOIR

Le cyber espace, initialement censé être un espace complètement libre, voir même anarchique, s'est tout de même vu assimilé par un système de contrôle à la hiérarchie et aux lois bien rigoureuses : le marché capitaliste d'une économie des données. Rappelons que la notion de « cyber espace », par moment désigné par le terme « monde ou espace numérique » réfère à l'ensemble de l'espace virtuel. Il s'agit d'un espace bien plus large que le simple internet sur lequel tous et toutes ont déjà navigué[147]. Le cyber espace est un monde riche et complexe dont l'expérience dépasse aujourd'hui les écrans et est de plus en plus liée à celle du monde naturel. On en fait l'expérience quotidienne à travers les multiples interactions qu'offrent les objets connectés qui peuplent le quotidien. Dans cette seconde section, on traite des structures qui contribuent à l'affaissement de la vie privée et contreviennent à la mise en place de processus de *privacy*. Deux structures sont présentées : d'abord la culture de surveillance telle qu'identifiée par Véliz, puis la construction panoptique du cyber espace.

[147] Lessig, *op. cit*., p.9

La culture de surveillance : surveiller et être surveillé

Selon Véliz, après la monétisation des données, la seconde raison à la source de la marchandisation des données est en lien avec les répercussions ayant suivi les attentats du 11 septembre. Elle rappelle qu'un peu avant cet événement tragique, plusieurs organismes de réglementation commençaient déjà à s'inquiéter des pratiques de collectes de données employées par les compagnies[148]. En 2000, un rapport de la Commission Fédérale de Commerce américaine déposé auprès du Congrès faisait état de plusieurs préoccupations concernant la protection de la vie privée sur Internet et suggérait de prendre des mesures législatives afin de protéger les informations des usagers[149]. Véliz fait l'hypothèse que, sans le 11 septembre, il y aurait peut-être des processus de *privacy* beaucoup plus développés dans le cyber espace aujourd'hui, mais que cette attaque terroriste a soudainement mis à l'arrière-plan tout discours sur la protection de la vie privée et fait basculer l'occident dans ce que plusieurs théoriciens qualifient une « culture de la surveillance »[150].

La culture de surveillance est à distinguer des concepts « d'État de surveillance » et de « société de surveillance. » Harcourt en fait état dans son ouvrage *Exposed*[151]. L'État de surveillance est dépeint comme un gouvernement aux technologies de surveillance extrêmement développées et utilisées sur sa propre population pour mieux la gouverner. Nous pouvons ici autant imaginer un État Léviathan agissant pour le bien commun ou un État à la *1984* de Orwell, exerçant un pouvoir tortionnaire sur ses sujets[152]. Or, critique Harcourt, la situation à laquelle nous faisons aujourd'hui face ne provient pas seulement des États et de leur surveillance, laissant croire que nous avons en fait dépassé l'État de surveillance[153]. La surveillance n'est pas seulement effectuée par une seule entité étatique, mais par un amalgame de différents acteurs : le gouvernement, les multinationales, les services de renseignement secret, les amis Facebook et le voisin conspirationniste.

David Lyon est en accord avec ce constat. Dans son article *Surveillance Culture : Engagement, Exposure, and Ethics in Digital Modernity*, le sociologue soutient que le monde est

[148] Véliz, *op. cit*., p. 40.
[149] *Ibid.,* p. 41.
[150] *Ibid.,* p.42.
[151] Harcourt, *op. cit*.
[152] *Ibid.,* p.55-56.
[153] *Ibid.,* p.62.

entré dans une « culture de la surveillance. » La particularité de la culture de surveillance, par rapport à une société ou un état de surveillance, est que les pratiques liées à la surveillance se sont tellement développées et ont tellement intégré le quotidien, les us et coutumes, que les personnes deviennent complices de leur propre surveillance et participent même activement à celle-ci. En effet, "as an increasing proportion of our social relationships is digitally mediated, subjects are involved, not merely as the target or bearers of surveillance, but as more-and-more knowledgeable and active participants"[154].

D'après Lyon, la surveillance est en quelque sorte devenue un mode de vie pour les citoyens qui s'y conforment, que ce soit de façon volontaire et consciente, ou non. Il identifie trois raisons qui expliqueraient le conformisme des gens à la culture de surveillance.[155] D'abord, la multiplication des outils de surveillance dans l'environnement aurait contribué à désensibiliser les gens à ces outils, développant une sorte de familiarité. La caméra dans le bus, dans le supermarché, devant la maison du voisin, la surveillance au travail, le radar sur la route, sont tant d'outils de surveillance qui font partie du quotidien de tout un chacun et qui éventuellement ont habitué les gens à se savoir continuellement potentiellement épiés, normalisant le fait de la surveillance[156]. Puis, tout comme Véliz, Lyon identifie la peur généralisée et entretenue depuis les attentats de 2001 à New York, comme une menace ayant servi à justifier les pratiques de surveillance[157]. « On vous surveille pour votre propre sécurité, » expliquent les autorités. Acceptant cette logique, personne ne remet en question la présence de caméras ou les contrôles identitaires ; les personnes se soumettent à la surveillance parce qu'elles désirent voir les autres surveillés également. Finalement, avec l'apogée de la connectivité et de l'ère du partage, les personnes ont développé un certain plaisir à se montrer aux autres. Surveiller et être surveillé seraient devenues des formes de divertissement, explique Lyon[158]. On pense évidemment aux nombreux réseaux sociaux sur lesquels les usagers exposent constamment leur quotidien, puis observent celui des autres à travers leurs écrans. Ce sont ces trois composantes : l'habitude, la peur et le plaisir, qui ont progressivement et collectivement internalisé une culture de surveillance chez les gens.

---

[154] David Lyon, « Surveillance culture: Engagement, exposure, and ethics in digital modernity », *International Journal of Communication* 11, nº February (2017): p.828.
[155] David Lyon, *op cit*, p.829.
[156] *Ibid*.
[157] *Ibid*.
[158] *Ibid*.

La surveillance ayant ainsi pénétré chaque facette de la vie sociale et intime, il ne s'agit plus seulement d'un état passif dans lequel les personnes se savent surveillées sans chercher à s'y opposer. La surveillance est à ce point intégrée dans l'imaginaire collectif que les gens participent maintenant activement à leur propre surveillance dans une forme autosurveillance réalisée via les outils technologiques à la mode : une montre calcule le nombre de pas effectués, donne le battement cardiaque ainsi que le taux d'oxygène dans le sang, une application informe du nombre de cycles de sommeil complétés et de la qualité de ces derniers, et enregistre chaque jour l'heure du couché et du réveil, tandis qu'une assistance vocale rappel de prendre une pause lorsque des signes de fatigue sont affichés au volant. Sous prétexte d'atteindre une plus grande connaissance de soi, afin de pouvoir mener une vie meilleure, surveiller son propre corps et esprit sont devenues pratiques courantes[159]. Toutefois prévient Lyon, parmi la multitude de données générées par ces pratiques d'autosurveillance dans le but d'atteindre le '*quantified-self*,' une infime partie est réellement rendue accessible aux usagers des objets connectés : "the vast majority of the data [ends] up in the databases of the wearable device corporations"[160]. Peu importe puisque dans une culture de la surveillance, cela va de soi. Les personnes, comme dans d'autres cultures, entretiennent des imaginaires partagés de ce qu'est la surveillance, avec toutes les normes sociales et pratiques qui y sont associées :

> Surveillance imaginaries are constructed through everyday involvement with surveillance as well as from news reports and popular media such as film and the Internet. They include the growing awareness that modern life is lived under surveillance, that this affects social relationships in many ways - for instance, Will my employer look at my antics on this Facebook page? - that the very idea of an expectation of privacy may be moot, and that everything from complacency to confrontation may be appropriate modes of responding to surveillance. Surveillance imaginaries offer not only a sense of what goes on - the *dynamics* of surveillance - but also a sense of how to evaluate and engage with it - the *duties* of surveillance. Such imaginaries, in turn, inform and animate surveillance practices; the two belong together. [161]

Comparant la situation actuelle au monde fictif imaginé par Orwell, Harcourt écrit "[it] is almost as if someone had learned from Orwell's greatest error"[162]. Selon lui, la dernière dimension

[159] *Ibid*., p.827.
[160] *Ibid*.
[161] *Ibid.*, p.829-830.
[162] Harcourt, *op. cit*., p.35.

identifiée par Lyon, celle du plaisir, est la clef du système Big Brother 2.0. Alors que, dans le roman d'Orwell, la stratégie d'oppression était de supprimer toute forme de désir ou de plaisir, c'est précisément ces deux éléments qui sont aujourd'hui au centre des pratiques d'autosurveillance des personnes. Il est en effet bien plus facile de dompter les gens au moyen de leurs passions qu'en essayant de briser ces dernières[163]. Les producteurs des outils de surveillance en sont bien conscients. Le modèle d'affaire de Facebook, remarque Harcourt, est dépendant du plaisir que prennent les utilisateurs à utiliser la plateforme, et donc du temps qu'ils y passent[164]. Susciter le plaisir des utilisateurs afin qu'ils reviennent consommer plus de contenu est un art que les compagnies maîtrisent si bien qu'on parle de plus en plus de problèmes de dépendance aux écrans résultant des mécanismes de renforcement addictif qu'utilisent les plateformes technologiques[165]. Il s'agit d'un cercle vicieux. En effet, plus les utilisateurs sont connectés longtemps, plus grand le nombre de données collectées sur ces derniers, et plus de données sont collectées meilleure est la capacité des plateformes à analyser les préférences de leurs utilisateurs, sans oublier la maximisation des revenus grâce au micro-ciblage publicitaire[166], cette dernière pratique qui consiste à envoyer des publicités personnalisées selon le profilage effectué sur les personnes. Les études ont par ailleurs démontré l'efficacité de ces publicités ciblées qui suscitent beaucoup plus de clics que les publicités génériques[167].

Voici donc le premier élément structurel qui affecte la vie privée. Nous sommes tombés dans une culture de la surveillance faisant en sorte que les pratiques de collecte massive de données sont peu contestées. En fait, les individus s'abandonnent en fait à ces dernières, exaltés à l'idée d'acquérir leur prochain gadget technologique, le plus récent dispositif de surveillance moderne sur le marché.

---

[163] *Ibid*.
[164] *Ibid.,* p.42.
[165] Christian Montag et al., « Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories », *International Journal of Environmental Research and Public Health* 16, nº 14 (2 juillet 2019), https://doi.org/10.3390/IJERPH16142612.
[166] Christian Montag et al., « Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories », *International Journal of Environmental Research and Public Health* 16, nº 14 (2 juillet 2019): p.4, https://doi.org/10.3390/IJERPH16142612.
[167] *Ibid.*

L'architecture du pouvoir moderne : le régime de visibilité des réseaux sociaux

La section précédente a introduit le concept de culture de surveillance, identifiant ses sources, les pratiques qui la composent et les dynamiques qui la maintiennent. Cette section traite quant à elle du concept d'exposition qui habite le monde numérique, et spécialement les réseaux sociaux. Nous reprenons l'argument de Tania Bucher selon lequel il existe dans cet espace un régime de visibilité garanti par architecture, creusant davantage les modalités de la surveillance moderne qui affectent la vie privée numérique.

L'ouvrage *Surveiller et punir* de Michel Foucault offre une analyse approfondie des structures de pouvoir et de répression, analysant les différentes techniques d'assujettissement des corps et des esprits. Foucault y présente notamment le panoptique, un modèle de prison imaginé par Bentham afin d'optimiser la surveillance des prisonniers. Il s'agit d'une construction cylindrique au centre de laquelle se trouve une tour. Les cellules de prisonniers longent les murs du cylindre, et font toutes face à la tour dans laquelle se situe le gardien, dont seule la silhouette est visible depuis les cellules, protégée du regard des détenus par des vitres teintées. L'efficacité de la surveillance réside dans le fait que les détenus sont constamment susceptibles d'être épiés par le gardien, sans jamais savoir si tel est le cas. La seule présence de la silhouette est suffisante pour insuffler l'impression constante de surveillance, que le gardien soit en train de ronfler ou jouer au solitaire. C'est une figure architecturale dont l'agencement particulier génère le pouvoir disciplinaire: « [un] assujettissement réel naît mécaniquement d'une relation fictive »[168]. En effet, l'état de visibilité permanent induit par l'organisation physique de l'espace assure le fonctionnement automatique du pouvoir.

Bucher présente une version revisitée l'organisation architecturale du pouvoir proposée par Foucault, mettant en évidence le régime de visibilité qui structure le diagramme de pouvoir des nouveaux médias. Elle s'intéresse spécifiquement à la façon dont les espaces tels que les prisons, les hôpitaux ou les réseaux sociaux sont toujours configurés de façon à rendre certaines choses visibles et d'autres non, selon des logiques bien spécifiques. Ces lieux sont selon elle des "spaces of 'constructed visibility'"[169]. Il en va de même pour le régime qui dicte la visibilité sur les réseaux sociaux indique Bucher. C'est toutefois un régime de visibilité aux modalités définies par

[168] Michel. Foucault, *Surveiller et punir : naissance de la prison*, Éditions G, 1993: p.236.
[169] Taina Bucher, « Want to be on the top? Algorithmic power and the threat of invisibility on Facebook », *New Media & Society* 14, nº 7 (avril 2012): p.1170. 1164-80, https://doi.org/10.1177/1461444812440159.

l'architecture *algorithmique*, qui y influence les pratiques sociales. Il s'agirait selon Bucher d'un renversement du régime de visibilité panoptique qui permet de garantir la structure de pouvoir en ligne. Effectivement, ce serait ici la peur de l'invisibilité - plutôt que la menace de la pleine visibilité - qui agirait comme moteur de la participation subjective à son propre assujettissement : "[the] problem as it appears is not the possibility of constantly being observed, but the possibility of constantly disappearing, of not being considered important enough"[170]. Sur les réseaux sociaux, l'espace de visibilité est à la fois limité et distribué de façon arbitraire par l'algorithme. Ainsi pour pouvoir être visible auprès des autres utilisateurs, le bon internaute doit se plier aux pratiques encouragées : gazouiller, « *liker* », partager et repartager, publier nouvelles, photographies et « *stories*. »

Dans cette structure, la visibilité a une fonction de récompense plutôt que de punition[171]. Mais le pouvoir disciplinaire y fonctionne tout aussi adéquatement puisqu'elle réussit à rendre responsables les sujets de leur propre comportement. La quête de la visibilité, ou la peur de l'invisibilité, entraînent le sujet à penser et agir d'une certaine façon : "through the means of correct training, subjects are governed as to reach their full potentiality as useful individuals"[172]. Or, comme établi précédemment, sur les plateformes en ligne, le « bon » utilisateur est celui qui participe, interagit, bref qui consomme le produit, laissant derrière lui une traînée de données. La réussite de cette architecture de pouvoir n'est exprimée plus candidement qu'à travers les mots des adolescents passés en entrevue par danah boyd : "If you're not on [social media], you don't exist"[173]. Succombant à la pression d'être vu, celle qui subit la menace d'invisibilité devient le principe de son propre assujettissement, multipliant les actions pour rester visible.

L'analyse des modalités de la visibilité de Bucher donne un outil additionnel pour comprendre comment s'opérationnalisent les dynamiques de surveillance et d'exposition de soi dans le cyber espace. La peur de ne pas être vu joue un rôle essentiel dans l'assujettissement des usagers qui interagissent sur les différentes plateformes sociales en ligne. Que faire toutefois de ceux qui utilisent les réseaux sociaux de façon passive, ceux qui observent silencieusement sans vraiment contribuer au contenu, ceux qui déroulent le fil d'actualité sans y publier et regardent les

[170] *Ibid*., p.1171.
[171] *Ibid*., p.1174.
[172] *Ibid*., p.1175.
[173] boyd et Marwick, *op. cit*., p.8.

« *stories* » sans y réagir avec l'un des émoticônes proposés ? Ces usagers « observateurs » répondent-ils également à la discipline panoptique ou bien sont-ils de « mauvais » usagers ?

Il s'avère que même l'usager passif répond à l'impératif imposé par le régime de visibilité. Parce que, si vouloir être visible est déjà un moteur puissant, pouvoir voir l'autre l'est possiblement tout autant. Bêtes sociales, si ce n'est pas pour s'exposer elles-mêmes, les personnes utilisent les réseaux sociaux pour profiter de la visibilité qu'ils ont sur l'autre. Peu importe qu'une personne utilise toutes les fonctionnalités de la plateforme ou non, elle génère tout de même une quantité généreuse de données et comme mentionné plus tôt : l'important est de garder les gens connectés le plus longtemps possible sur la plateforme. Et cela fonctionne. En 2018, Statistique Canada recense que 77% des Canadiens utilisent régulièrement les réseaux sociaux[174]. Cette statistique monte à plus de 90% pour les tranches d'âge de 15 à 34 ans. C'est peut-être là le tour le plus ingénieux de ce système : le spectacle numérique est à la fois produit et consommé par les usagers.

L'infosphère numérique en question

Jusqu'à présent nous nous sommes intéressés aux structures et dynamiques socio-économiques en place dans le monde numérique qui participent au détriment de la vie privée; la culture de surveillance et le régime de visibilité. Sous ces structures de pouvoir, il y a pourtant un environnement extrêmement malléable dont les règles peuvent être complètement changées. La théorie de l'information de Floridi nous aide à comprendre comment s'articulent les flux d'informations dans le monde numérique, et conclut notre démonstration de l'érosion de la vie privée en ligne.

Reprenant la théorie de l'information de Floridi, on peut considérer le monde comme une « infosphère », soit un espace dans lequel des agents informationnels reçoivent et transmettent de l'information[175]. Simplifiant le modèle pour les fins de compréhension, il imagine un domaine délimité dans laquelle interagissent des agents informationnels. Il prend l'exemple d'une maison dans laquelle des personnes sont dans différentes pièces[176]. L'ontologie (la nature) de l'environnement informationnel, explique Floridi, dépend des propriétés de cet espace et des

[174] Statistique Canada, « Canadian's assessments of social media in their lives », 2018, https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm.
[175] Floridi, "The ontological interpretation of informational privacy", *op. cit*.
[176] *Ibid.*, p.188.

agents qui s'y trouvent. Le « *gap* informationnel » entre les agents est une fonction du degré d'accessibilité des informations. Le niveau d'accessibilité de l'information est quant à lui un facteur épistémique dépendant des caractéristiques ontologiques de l'infosphère. Floridi explique que l'accessibilité informationnelle sera plus ou moins grande "depending on whether the [agents] are allowed, e.g., to have their own rooms and lock their doors"[177], mais également "on the ontological features of the infosphere, i.e. on the nature of the specific agents, of the specific environment, […]"[178]. Par exemple, des murs en béton insonorisé réduisent l'accessibilité alors que des murs en verre translucide l'augmentent. Les caractéristiques ontologiques de l'infosphère déterminent le degré de « friction ontologique » qui régule le flux d'information dans l'environnement. Ici, "ontological friction refers here to the forces that oppose the information flow within (a region of) the infosphère, and hence (as a coefficient) to the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment"[179].

Dans son article de 2005 décrivant sa théorie informationnelle, Floridi propose de concevoir l'influence des nouvelles technologies de l'information comme une '*re-ontologization*' de l'infosphère[180]. La numérisation de l'environnement informationnel, l'augmentation de la puissance des ordinateurs, les objets connectés, tous ces éléments influencent les caractéristiques ontologiques de notre infosphère et influencent donc également la friction ontologique dans le cyber espace. À l'époque, Floridi n'émet pas d'hypothèse à savoir si la friction ontologique de l'environnement informationnel s'est vue augmentée ou diminuée par ces changements, il indique seulement que ces certaines de ces nouvelles technologies peuvent améliorer la *privacy* informationnelle et d'autres la réduire. La proposition mise de l'avant dans notre chapitre est que les nouvelles technologies de l'information, et plus spécifiquement la numérisation des données ont réduit la *privacy* informationnelle des agents. Pour conclure cette démonstration, nous proposons maintenant de reprendre la définition de vie privée établie au premier chapitre et de l'intégrer au modèle de Floridi, mettant en lumière l'absence de *privacy* informationnelle dans l'infosphère numérique.

[177] *Ibid.*, p.186.
[178] *Ibid.*
[179] *Ibid*.
[180] *Ibid.*, p.188.

Nous avons défini la vie privée comme étant « *l'ensemble des processus et stratégies par lesquels les individus essaient de rendre leur personne ou leurs relations intimes inaccessibles aux autres.* » Nous avons également établi que parmi les processus *privacy* possibles, certains dépendent des individus, comme les processus verbaux et comportementaux qui sont mis en place par les personnes, alors que les autres mécanismes ne relèvent pas nécessairement de ces dernières. En effet, les mécanismes sociaux relèvent des normes sociales en place alors que les mécanismes environnementaux relèvent en partie des individus (mettre des rideaux sur ses fenêtres), mais également des structures publiques en place (le bureau du médecin ou les cabines téléphoniques). Dans le contexte de l'infosphère numérique qui est celle du Cyberespace, les moyens de *privacy* disponibles sont certainement dépendants des caractéristiques ontologiques de l'infosphère en question. Or ce que le dernier chapitre a démontré est que les caractéristiques de l'infosphère actuelle provoquent d'une part des frictions ontologiques asymétriques et limitent d'autre part les moyens de *privacy*.

Il existe dans l'infosphère numérique, on peut considérer qu'il y a globalement une faible friction ontologique. La numérisation de l'information et la grande connectivité ont en effet contribué à faciliter la circulation de l'information, notamment entre les usagers du cyberespace. En fait, la mise en circulation d'information par les personnes est même encouragée par la culture de surveillance et une tendance à l'exposition de soi découlant du régime de visibilité. De plus, il y a une très faible friction ontologique dans le flux d'information allant des individus vers les organisations propriétaires des technologies de l'information. Ces dernières peuvent être considérées comme un second type d'agents informationnels dans notre modèle puisque qu'elles agissent comme tel; captant et produisant de l'information. Toutefois, il y a une asymétrie flagrante dans le degré de friction ontologique des flux informationnels entre ces deux types d'agents informationnels. Les organisations comme les GAFAM[181] ont un accès inestimable à l'information produite par les personnes via les différents objets connectés, *cookies*, et autres outils de collectes d'information. Elles peuvent également transmettre de l'information vers les personnes (comme leurs publicités ciblées), mais ont en revanche un bien meilleur contrôle sur l'accès à l'information

[181] Cet acronyme réfère aux cinq plus grandes compagnie de tech (en valeur boursière), soit Google, Apple, Facebook, Amazon et Microsoft. Mais plusieurs autres compagnies pourraient être ajoutée à cette liste : Alibaba, Samsung, Netflix, et bien d'autres encore.

qu'elles produisent via leur contrôle des outils technologiques comme les algorithmes. Contrôle que les personnes n'ont pas en raison du manque de moyens de *privacy* qui leur sont disponibles.

En ce qui concerne les processus de privacy, très peu sont disponibles aux personnes dans l'infosphère numérique. D'abord, le manque de littératie numérique rend difficile l'adoption de stratégies de *privacy*[182]. En effet, à moins d'être familier avec la programmation et donc le fonctionnement du cyberespace, l'accessibilité à des moyens de *privacy* efficaces est compliquée, voire impossible. Ensuite, en ce qui concerne les processus de *privacy* culturels, ils sont également inexistants comme nous l'a appris l'analyse sur la culture de surveillance en place dans le cyberespace. Voici donc le constat du présent chapitre : dans l'infosphère du cyberespace, il n'y a présentement aucune friction ontologique. L'information y circule sans aucune peine tant l'environnement est friable, mais de façon asymétrique et au profit de certains agents informationnels seulement.

Changer le code

Le cyberespace est rempli d'architectures de visibilité, qu'elles soient structurelles via les caractéristiques de l'environnement numérique, ou encore social à travers les dynamiques et pratiques culturelles qui y prennent part. Pourtant, rappelle Lessig, l'environnement numérique est un endroit complètement malléable dans lequel les problèmes, lorsqu'identifiés comme tels, peuvent littéralement être « '*coded' away* »[183]. Voici la note sur laquelle se conclut ce chapitre. Reposant sous les structures de pouvoir en place, des mécanismes sociaux et des intérêts économiques, le cyberespace demeure une structure malléable[184]. Dans ce contexte, on ne peut prétendre à une neutralité technologique. Le design des technologies étant toujours imprégné des valeurs et du sens normatif que les concepteurs lui ont donné, il n'est jamais neutre. Les technologies peuvent néanmoins être remodelées pour refléter, non pas les valeurs économiques ou celles du pouvoir, mais celles choisies en société[185]. Voici le plaidoyer normatif qui motive ce mémoire : la vie privée numérique devrait être une valeur privilégiée dans le contexte actuel et la *privacy* informationnelle devrait être intégrée par design dans l'architecture du cyberespace. Le

[182] Frank Pasquale, *The Black Box Society : The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015): p.54.
[183] Lessig, *op.cit*., p.15.
[184] *Ibid.*, p.32.
[185] *Ibid.*

prochain chapitre poursuit en ce sens en présentant un argument moral qui justifie l'importance de la vie privée numérique et adresse certains mythes et débats en lien avec la vie privée numérique.

Pour vivre heureux, vivons cachés

Adage populaire

CHAPITRE 3 : VERS UNE MEILLEURE DÉFENSE DE LA VIE PRIVÉE

Les sociétés libérales, fondées sur des principes de justice équitables, et reconnaissant aux personnes des droits et libertés intrinsèques destinés à assurer leur protection et leur épanouissement, peuvent et doivent se doter des moyens nécessaires à l'atteinte des objectifs qu'elles se sont démocratiquement choisis. Le processus démocratique implique une délibération publique permettant de négocier, en société, les finalités et priorités à fixer. En outre, les sociétés sont souvent aux prises avec des conflits de valeurs. Il faut régulièrement choisir un certain équilibre entre des valeurs diamétralement opposées, par exemple entre l'idéal de la transparence comme gage d'honnêteté et le respect de l'intimité, entre une plus grande sécurité publique et le respect de la vie privée. Aussi la vie privée est une valeur périodiquement remise en question selon les enjeux particuliers de l'époque et la société, au profit d'autres idéaux tels que la sécurité publique, la transparence, ou l'accès à l'information. Alors que les sociétés se questionnent sur ces différents enjeux, les sciences sociales sont bien placées pour analyser ces catégories et valeurs en cours de redéfinition et fournir des fondements théoriques et arguments moraux sur lesquels asseoir le débat. Ce chapitre a pour ambition de fournir un tel cadre théorique, et plus particulièrement, d'offrir les arguments éthiques nécessaires à la défense de la vie privée dans le contexte numérique.

Dans le premier chapitre, la définition de la vie privée a été établie de façon purement descriptive. Cet exercice de délimitation conceptuel a permis d'identifier les thèmes et éléments importants liés à la vie privée, comme les différents processus de régulation de l'accès à soi. Ce premier chapitre avait pour conclusion que la possibilité d'avoir et de maintenir une vie privée demande nécessairement qu'il y ait des processus de *privacy* à la disposition des personnes, ou intégrés à même l'environnement quand celui-ci est public. En effet, être dans une situation de vie privée effective signifie en d'autres termes avoir des processus de *privacy* suffisants en place afin de réguler l'accès à soi. Le deuxième chapitre a ensuite permis d'expliquer en quoi l'univers numérique, en raison de la valorisation des données et des structures de surveillance en place, ne

permet peu ou pas de processus de *privacy*. Il n'y a pas, ou presque pas, de vie privée possible dans le monde numérique.

Ce troisième et dernier chapitre reprend la notion de vie privée, et plus particulièrement la vie privée numérique, mais avec, cette fois-ci, une ambition normative. L'objectif de ce chapitre est de présenter une justification morale en faveur de la protection de la vie privée numérique et ainsi faire un plaidoyer pour de meilleurs et plus nombreux processus de *privacy* numériques. Il s'agira en premier lieu de déconstruire certains des discours présentement utilisés pour minimiser les enjeux liés à la vie privée ou encore les contourner. Nous traiterons d'abord du mythe du '*privacy paradox*'[186] puis de l'utilisation fautive du consentement comme moyen de renoncer à la vie privée numérique. Dans un second temps, nous démontrons pourquoi il est moralement important de garantir des processus de *privacy* aux personnes dans le contexte particulier qui est celui du monde numérique. En effet, devant les enjeux que soulève ce dernier, il convient de revisiter les différents arguments en faveur d'une protection de la vie privée afin de rappeler l'importance de celle-ci, mais surtout, d'outiller les revendications, présentes et futures, pour que de meilleurs processus de régulation de l'accès aux personnes soient mis en place et accessible. Le chapitre se conclut sur la thèse principale de notre mémoire : selon nous, la mise en place des processus de *privacy* doit être un projet de société puisque cette responsabilité ne peut incomber uniquement aux individus.

DÉCONSTRUIRE LES DISCOURS « ANTI-PRIVACY »

Afin de faire une défense adéquate de la vie privée comme valeur à adopter en société, il faut s'intéresser aux discours et arguments qui participent à sa remise en question. Il y en a deux qui occupent particulièrement de place les débats publics et qu'il nous faut absolument aborder et déconstruire. C'est donc ce que nous ferons dans la première moitié de ce chapitre.

Le mythe du Privacy Paradox

L'importance donnée à la vie privée varie d'une personne, d'une société et d'une époque à l'autre. Il peut même par moment y avoir des combats de valeurs entre la vie privée, et d'autres priorités telles que la sécurité. Nous pensons par exemple aux bouleversements dans les politiques

[186] Solove, « The Myth of the Privacy Paradox ».

et discours publics qui ont suivi les attentats du 11 septembre alors que la vie privée a été reléguée au second plan en faveur de mesures de sécurité publique rehaussées. La culture de *privacy* d'une société peut donc vraisemblablement changer. Nous pouvons également penser à la culture de surveillance et la tendance à l'exposition de soi présentée au second chapitre qui ont changé les mœurs des personnes, diminuant (en apparence du moins) l'importance donnée à la vie privée. Ce que cette analyse peut porter à croire est que les gens ne se soucient plus vraiment de leur vie privée puisqu'ils participent à leur propre surveillance et s'exposent même. Mais dans ce cas, comment expliquer qu'encore à ce jour 92% des Canadiens indiquent être à tout le moins « quelque peu préoccupés par la protection de leur vie privée » et près de 60% des Canadiens se disent « préoccupés » ou « énormément préoccupés » par cet enjeu[187]. C'est ce qui est appelé le '*privacy paradox*': "the phenomenon where people say that they value privacy highly, yet in their behavior relinquish their personal data for very little in exchange or fail to use measures to protect their privacy"[188].

Le *privacy paradox*, indique Daniel Solove, est la source d'une littérature abondante et joue un rôle important dans les débats sur la vie privée et la manière dont elle devrait être réglementée [189]. De nombreuses études empiriques ont été menées pour essayer de comprendre l'incohérence entre les positions déclarées en matière de protection de la vie privée et le comportement des gens lorsqu'il a trait au partage de données. Deux explications du soi-disant paradoxe s'opposent et dominent la littérature[190].

La première prend une approche empirique, affirmant que le comportement est un indicateur plus fiable de la valeur que les gens accordent à leur vie privée que les déclarations de principe faites par ces derniers[191]. Le paradoxe s'expliquerait donc ainsi : ce que les personnes affirment sur la valeur qu'elles accordent à la vie privée n'est pas représentatif de leur réelle croyance; leur comportement révèle qu'ils accordent une faible valeur à leur vie privée. Cette évaluation du comportement comme révélatrice des positions sur la vie privée aboutit souvent à

[187] Commissariat à la protection de la vie privée du Canada, « Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019 », s. d., https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/#fig03.
[188] Solove, "The Myth of the Privacy Paradox.", *op. cit.*, p.2.
[189] *Ibid*., p.3.
[190] *Ibid*.
[191] *Ibid*., p.11-12.

des affirmations problématiques sur la valeur de la vie privée, par exemple que la vie privée n'est pas importante aux yeux des gens et donc qu'il n'est pas nécessaire de fournir des mesures additionnelles de protection[192]. Solove explique que ces affirmations sont basées sur une série de généralisations abusives sur le comportement des gens. En effet, cet argument généralise les préférences des personnes dans des contextes bien spécifiques de partage des données pour en tirer des conclusions grossières sur la valeur que les gens accordent à leur vie privée numérique[193].

La seconde explication au paradoxe adopte la logique inverse. Elle utilise l'argument de « distorsion du comportement », soit que le comportement des personnes est irrationnel ou non conforme à leurs préférences réelles[194]. Comme les sciences économiques l'ont démontré, plusieurs problèmes de prise de décision s'expliqueraient par des heuristiques biaisées et des préjugés qui faussent la capacité des gens à évaluer leurs options de manière rationnelle, d'où les comportements irrationnels[195]. Par exemple, dans le cas du partage de données : "people are more comfortable supplying personal data when they feel in control—even if that control is illusory"[196]. Un autre argument en faveur de cette thèse est que le comportement des personnes est manipulé par les entreprises et influencé par le design technologique. En effet, les nouvelles technologies sont souvent conçues pour maximiser la collecte de données et pousser les gens à adopter certains comportements qui favorisent cette collecte[197]. Un facteur additionnel résiderait dans le manque de connaissance et les incompréhensions des gens face aux technologies et les conséquences réelles sur leur vie privée[198]. Ainsi, pour évaluer la valeur réelle accordée à la vie privée, ce ne serait donc pas les comportements des personnes qu'il faut considérer, mais bien leur discours sur leurs préférences.

En somme, explique Solove, "[the] behavior distortion argument demonstrates that behavior is extremely malleable and thus offers a compelling case for explaining why behavior is not a reliable metric for people's actual attitudes about privacy"[199]. Pour cette raison, nous sommes de l'avis de Solove qui juge cette seconde explication plus convaincante que la première. Or,

[192] *Ibid*., p.23.
[193] *Ibid*.
[194] *Ibid*., p.15.
[195] *Ibid*., p.16.
[196] *Ibid*., p.17.
[197] *Ibid*., p.18.
[198] *Ibid*., p.19.
[199] *Ibid*., p.22.

Solove pousse encore plus loin la réflexion sur le *privacy paradox,* affirmant qu'il n'en est pas un, mais plutôt l'illusion d'un paradoxe engendrée par une logique fautive[200].

Le problème du *privacy paradoxe* repose sur l'idée que les gens accordent une valeur déterminée à la vie privée, que l'on tente d'établir sur la base de leurs comportements et préférences. Solove remet toutefois cette prémisse en question : "[whether] measured via stated attitudes or behavior, preferences themselves are not static; they are highly contextual, subject to distortion, and malleable"[201]. Selon Solove, le paradoxe n'existe pas. En effet, le "paradoxe" se trompe sur la signification des comportements comme celui de choisir un service moins cher, mais qui collecte plus d'informations personnelles. Ces comportements ne sont pas le reflet des valeurs des personnes, explique Solove, mais plutôt de leur perception du risque dans des contextes spécifiques[202]. Aussi, que les gens partagent leurs livres ou films préférés, leurs croyances religieuses et convictions politiques ou encore des moments de leur quotidien par image ou vidéo sur les plateformes en ligne, n'est pas nécessairement synonyme d'une faible attention à leur vie privée. Une personne peut être très préoccupée par l'utilisation néfaste de ces données personnelles, mais ne pas percevoir ou sous-évaluer le risque du partage de ces informations dans un contexte donné.

Si l'on peut tirer une conclusion de ces comportements d'exposition, ce n'est pas que les personnes accordent telle ou telle valeur à la vie privée ou encore à leurs données; "[instead], the main conclusion is that in a particular context when data is provided to a particular entity, a person is assessing the risk of undesirable uses as lower than the particular monetary reward"[203]. Il ne s'agit donc pas d'une question de valeur ici, mais bien d'évaluations des risques (des coûts et bénéfices) dans un contexte particulier dans lequel les agents décisionnels possèdent par ailleurs des informations limitées et peuvent être influencés par des biais ou un design technologique persuasif, voir trompeur. En somme, l'article de Solove démontre que le comportement des gens dans un contexte spécifique n'est pas une indication significative de la valeur que les gens accordent à la vie privée et encore moins de la valeur que la société devrait accorder à la vie

[200] *Ibid*., p.4.
[201] *Ibid*., p.22.
[202] *Ibid*., p.24.
[203] *Ibid*., p.27.

privée: "privacy's value is as a constitutive element in society, not a bartered good in the marketplace"[204].

Solove fait remarquer que si le privacy paradoxe n'est pas un paradoxe, nous pouvons tout de même tirer des conclusions intéressantes des comportements exhibés par les personnes en ligne. Le comportement des gens témoigne globalement de leur incapacité à protéger adéquatement leur vie privée numérique et de leur disposition à partager leurs données personnelles sans hésitation[205]. En fait, il n'est pas étonnant de constater l'incapacité des gens à gérer efficacement leur vie privée numérique tant cette gestion est ardue :

> Privacy self-management involves the various decisions people must make about their privacy and the tasks people are given the choice to do regarding their privacy, such as reading privacy policies, opting out, changing privacy settings, and so on. Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively. The best people can do is manage their privacy haphazardly. People cannot learn enough about privacy risks to make informed decisions about their privacy. People will never gain sufficient knowledge of the ways in which personal data will be combined, aggregated, and analyzed over the years by thousands of organizations. Resignation is a rational response to the impossibility of privacy self-management.[206]

Il faut lire ici que la gestion des stratégies de *privacy* dans le monde numérique est complexe et que la prise en charge individuelle de ces stratégies est presque impossible. La prochaine section explore précisément l'un des stratagèmes qui contribuent à ce que les personnes soient limitées dans leurs stratégies *privacy* en ligne.

Renoncer à sa vie privée ? La question du consentement

Un débat commun sur la question de la légitimité de la collecte et de l'utilisation des données par les GAFAM est celui du consentement des utilisateurs[207]. À la fois les GAFAM et les défenseurs de la vie privée utilisent la notion de consentement pour justifier leurs pratiques d'une

[204] *Ibid*., p.5.
[205] *Ibid*., p.33.
[206] *Ibid*., p.5.
[207] Elettra Bietti, « The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond », *Stanford University Aegis Paper Series*, nº 2001 (2020).

part[208], et renforcer les régulations en place de l'autre[209]. En effet, les grandes entreprises tech prétendent être légitimes dans leurs pratiques de traitement des données puisqu'ils affirment obtenir préalablement le consentement de leurs utilisateurs. De l'autre côté, les nouvelles régulations misent en place pour protéger les droits des utilisateurs, notamment celui à la vie privée et à la protection des données, reposent largement sur la notion de consentement dans l'objectif de permettre aux utilisateurs d'être en meilleure posture vis-à-vis des géants[210]. On peut difficilement s'attaquer à la question de la protection de la vie privée sans se pencher sur ce débat. L'objectif ici n'est pas de questionner la légitimité légale de telle ou telle pratique ni la force normative des lois et règlements mis en place. Il s'agit plutôt de remettre en question la valeur morale du consentement dans le cadre de l'utilisation des outils numériques. En effet, si on désire défendre une meilleure protection de la vie privée en ligne, il faut répondre à la question à savoir si, d'un point de vue éthique, les personnes renoncent effectivement à leur vie privée en consentant aux termes des compagnies tech. Si c'est effectivement le cas, l'ensemble du présent projet se résumera à un appel à prudence et à la conscientisation des individus relativement à leurs pratiques en ligne. Or, il est de l'avis de l'auteur que le consentement des utilisateurs n'est ni libre, ni éclairé, et que, en appuyant sur « s'inscrire, » (voir *Figure 1*) les personnes ne consentent pas en bonne et due forme à voir leurs données personnelles accaparées par les fournisseurs de services numériques.

Les utilisateurs des différents outils technologiques, lorsqu'ils décident d'utiliser l'outil, acceptent les conditions d'utilisation de ce dernier. L'utilisateur qui s'inscrit sur une application comme Facebook doit consentir aux conditions d'utilisations de la plateforme. Ainsi, lorsque les GAFAM sont accusées de pratiques abusives de collecte et minage de données, elles se défendent en disant qu'elles ont l'autorisation (le consentement) de leurs utilisateurs [211]. On peut notamment lire dans celles de Facebook :

> Nous recueillons le contenu, les communications ainsi que d'autres informations que vous fournissez lorsque vous utilisez nos Produits, notamment lorsque vous créez un compte, lorsque vous créez ou partagez du contenu, ou lorsque vous communiquez avec d'autres personnes ou leur envoyez des messages. Cela peut comprendre des informations présentes dans le contenu que vous fournissez (par exemple, des

[208] Elizabeth Schulze, « Facebook says it got users' permission to share data - users disagree », *CNBC*, décembre 2018.
[209] Bietti, *op cit*, p.1
[210] *Ibid*.
[211] Schulze, *op. cit*.

métadonnées) ou concernant un tel contenu, tel que le lieu d'une photo ou la date à laquelle un fichier a été crée.[212]

Du côté des initiatives de régulation, il y a un engouement visible pour les stratégies d'« autogestion de la vie privée » (*privacy self-management*), soit un contrôle et un choix individuel sur l'utilisation de ses données et les paramètres de confidentialité souhaités. Le RGPD entré en vigueur en 2018 repose par exemple largement sur les concepts de contrôle et de consentement des utilisateurs [213]. Pourtant, il y a un scepticisme croissant dans les cercles académiques quant à l'efficacité et du consentement dans le contexte du traitement de données personnelles [214]. Schermer et ses co-auteurs remarquent que « [as] it stands, there seems to be a

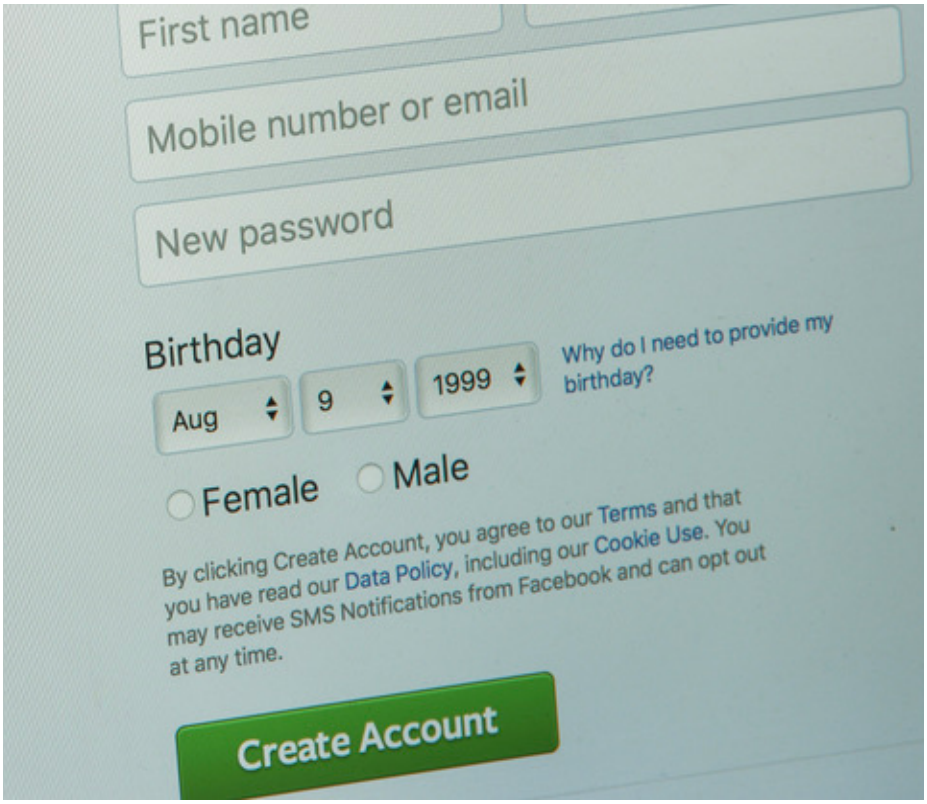

Figure 1 - Facebook website homepage (image libre de droit téléchargée sur shutterstock .com)

[212] Consulter « Politique d'utilisation des données » de Facebook, https://www.facebook.com/about/privacy/update/printable

[213] Réglement Générale sur la protection des données (GDPR), Journal officiel de l'Union européenne, 27 Avril 2016 (L 119), Article 7.

[214] Bart W Schermer, Bart Custers, et Simone Van Der Hof, « The crisis of consent: how stronger legal protection may lead to weaker consent in data protection », *Ethics and Information Technology* 16 (2014), https://doi.org/10.1007/s10676-014-9343-8.

disconnect between the legal theory, which presupposes a rational, informed data subject who makes conscious decisions, and the current practice in which data subjects simply agree to almost all consent requests without actually reading the fine print »[215]. La *Figure 1,* page d'inscription à partir de laquelle une personne peut s'abonner en un seul *click* à l'application Facebook (et accepte par ce même clic l'ensemble des conditions d'utilisation), illustre bien la facilité et la rapidité du consentement sur cette plateforme.

Le consentement, outre son rôle contractuel dans les sphères institutionnalisées, exerce d'abord et avant tout un rôle moral hors du commun dans le contexte social [216]. Kleinig réfère à la « magie morale » du consentement [217]. Le consentement est un acte moralement transformateur qui modifie les attentes normatives entre les personnes et les groupes [218]. En effet, le consentement peut générer une permission qui autorise, dans un certain cadre, quelqu'un d'autre de faire ce qui serait autrement considéré comme un acte moralement illicite. Ainsi le consentement peut apparaître comme un acte de magie puisque par cette simple formule « je consens », ce qui était interdit est soudainement autorisé. Toutefois, pour que la magie morale du consentement puisse s'opérer de façon légitime, un nombre de critères doit être respecté, sans quoi la valeur du consentement ne peut être moralement légitime. C'est donc le respect de ces critères qui confère la valeur au consentement. La nature et le nombre exact d'exigences varient d'une théorie morale à l'autre, mais Kleinig en identifie quatre qui semblent assez universels [219].

D'abord, la personne (ou le groupe) qui consent doit être compétent, soit avoir les capacités cognitives suffisantes pour être en mesure d'effectuer une évaluation rationnelle des implications de l'objet consenti [220]. Une personne intoxiquée, ou un jeune enfant pourraient par exemple ne pas répondre à cette exigence. Cela dépendra toutefois de la nature de la transaction; le niveau de compétence pouvant varier qu'il s'agisse de rejoindre un club sportif ou bien faire l'achat d'une maison [221]. Deuxièmement, le consentement doit être fait volontairement, c'est-à-dire dans

[215] *Ibid*., p.171.
[216]John Kleinig, « The Nature of Consent », in *The Ethics of Consent : Theory and Practice*, éd. par Franlklin G Miller et Alan Wertheimer, Oxford University Press, 2010: p.4, https://doi.org/10.1080/00455091.1982.10715825.
[217] *Ibid*.
[218] *Ibid*.
[219] *Ibid*., p.13; Schermer et al., *op cit*., p.172.
[220] Kleinig, *op cit*., p.13-14.
[221] *Ibid*., p.13.

l'absence de coercition [222]. La coercition, remarque Kleinig prend traditionnellement la forme d'une menace, mais peut selon lui également résider dans le simple contexte dans lequel l'entente prend place : "[if] a factory owner takes advantage of economic conditions to advertise a subsistence wage for heavy work, we may see the offer as genuine but coercive"[223]. Ensuite, il y a une condition de connaissance. La partie qui consent doit le faire en connaissance de cause : elle doit être en possession des informations nécessaires pour prendre une décision éclairée [224]. Selon Kleinig, cette troisième condition requiert un minimum de responsabilité de la part de celui qui consent[225]. Ce dernier doit faire un effort suffisant pour s'informer correctement, sans quoi son consentement est certes mal informé, mais néanmoins valide. Finalement, le critère d'intention prévoit que l'objectif final derrière l'objet de l'accord soit clarifié [226]. En effet, si A consent à prêter sa voiture à B et que B utilise celle-ci pour voler une banque, il ne s'en suit pas que A a consenti à cet usage du véhicule[227]. Ce dernier critère est particulièrement important puisqu'il prévient que le consentement soit utilisé comme une forme de « carte blanche. »

Sans le respect plein et entier de l'ensemble de ces conditions, le consentement n'est pas doté de son pouvoir moralement transformatif. Maintenant, qu'en est-il du consentement donné aux plateformes numériques par leurs utilisateurs? Supposant que la majorité des utilisateurs des outils numériques soient effectivement compétents, il reste à vérifier si les trois autres conditions sont également remplies.

En ce qui concerne la condition de non-coercition, le contexte de monopole des GAFAM sur le marché porte à croire que le cadre dans lequel se tient la transaction exerce une pression sur les utilisateurs. En effet, les sociétés modernes sont à ce point dépendantes des technologies, que même le technophobe détient fort probablement sa propre traînée numérique. Les outils technologiques offerts par les GAFAM sont tellement présents dans le quotidien, que refuser leur utilisation comporte aujourd'hui un coût social et d'opportunité beaucoup trop élevé pour la plupart des gens. Un étudiant se coupera-t-il de toutes les activités sociales et associatives de son programme d'étude parce que la plateforme utilisée par les groupes universitaires pose des enjeux

[222] *Ibid*., pp.14-15.
[223] *Ibid*., pp.15-16.
[224] *Ibid*., pp.16-17.
[225] *Ibid*., p.16.
[226] *Ibid*., p.17-20.
[227] *Ibid*., p.17-18.

de vie privée? Est-ce qu'une personne sera prête à refuser une offre d'emploi parce que le système de messagerie utilisé par cet employé est hébergé chez Google ou Microsoft? Une entrepreneure renoncera à afficher son commerce sur Facebook et Instagram, sachant qu'elle se prive ainsi de la visibilité requise pour développer son entreprise? Est-ce que les activistes, personnalités politiques, philosophes et autres influenceurs de ce monde cesseront de diffuser leurs convictions et enseignements faute de meilleurs moyens de protection que l'autocensure numérique? La possibilité de faire un choix *volontaire* (et non imposé) repose selon Frank Pasquale sur l'existence d'options multiples uniquement possible dans un marché numérique compétitif[228]. Or, le monopole des GAFAM rend extrêmement difficile le développement d'outils numériques alternatifs intéressants. Cédant aux forces d'un marché dans lequel les données massives sont la clef de la maximisation du profit, toute entreprise a intérêt à exploiter les données, ce qui contrevient au développement d'alternatives protégeant la vie privée par d'éventuels compétiteurs[229]. Bref, le consentement des usagers est à plusieurs égards donné dans un contexte de coercition.

Selon le cadre normatif entourant le concept de consentement développé par Kleinig, cette dernière conclusion est à elle seule suffisante pour réfuter la légitimité morale du consentement donné par les utilisateurs des applications numériques. Les deux dernières conditions permettent toutefois de renforcer l'argument. Concernant l'exigence d'information, on rappelle que selon Kleinig, la responsabilité de s'informer correctement incombe à la personne qui doit donner son consentement. Ce que Kleinig omet de préciser est le degré de cette responsabilité. D'autres théoriciens ont commencé à traiter du phénomène de « surcharge de transactions de consentements »[230]. En pratique, explique Schermer, "there are simply too many consent requests for an individual user to consider, watering down the psychological effect of being confronted with a consent transaction"[231]. Ce faisant, l'utilité effective et la valeur morale du consentement se retrouvent noyées par sa surutilisation, portant à contester la légitimité du fardeau d'information qui repose supposément sur l'utilisateur. Ensuite, en ce qui a trait à la clarté de l'intention réelle vis-à-vis de l'objet de la transaction, bien que les conditions d'utilisation offrent une idée générale du type de données collectées et des usages que compte en faire la compagnie, il existe une grande opacité entourant les détails de l'utilisation des données. Par exemple, Facebook explique dans ces

[228] Pasquale, *op cit*, p.81.
[229] *Ibid*.
[230] Schermer, *op cit*, p.176.
[231] *Ibid*.

termes d'usage que les données récoltées sur les utilisateurs sont notamment utilisées pour « personnaliser les fonctionnalités et le contenu » ou encore « faire des suggestions […] susceptibles de vous intéresser. »[232] Il n'est toutefois pas question du traitement des données par leurs algorithmes ni des expériences conduites dans le laboratoire vivant que représente la plateforme. En 2012, des scientifiques de Facebook ont réalisé une expérience sur les utilisateurs visant à tester si l'humeur des utilisateurs était influencée par celle de leurs « amis » Facebook :

> The Facebook researchers […] ran the experiment on 689,003 Facebook users. (The users, incidentally, did not know they were being experimented on, nor had they given informed consent. Facebook's view was that they had implicitly consented when they originally agreed to Facebook's term of service. Facebook apparently "argued that its 1.28 billion monthly users gave blanket consent to the company's research as a condition of using the service)[233]

Il semble effectivement y avoir un abus de la part des GAFAM en ce qui concerne l'utilisation du consentement de leurs utilisateurs. Donner son consentement à un moment *T* pour une utilisation particulière de ses données ne donne par carte blanche pour en faire tout et n'importe quoi par la suite. À la lumière de cette analyse, force est de constater que le soi-disant consentement donner par les utilisateurs n'est pas moralement valide. En fait, on peut complètement remettre en question la valeur du consentement des utilisateurs comme principal moyen de contrôle sur l'accès aux données personnelles. Le simple fait d'être invité à consentir à une pratique ne donne pas aux individus un droit de regard significatif sur cette pratique et ne leur donne pas la possibilité de choisir des options alternatives[234].

Ce que les deux dernières sections ont notamment servi à démontrer est que le fardeau des mesures de protections de la vie privée numériques et la responsabilité de revendiquer son désir de *privacy* par ses dernières reposent largement sur les individus. Nous sommes d'avis que cette attitude face à la vie privée numérique est vouée à l'échec puisque les conditions actuelles sont incompatibles à tout projet de vie privée numérique. La prochaine section fait un plaidoyer en faveur d'une meilleure protection de la vie privée par la voie de moyens *collectifs*.

[232] Consulter « Politique d'utilisation des données » de Facebook, https://www.facebook.com/about/privacy/update/printable
[233] Harcourt, *op cit*, p.42.
[234] Bietti, *op cit*, p.3.

FONDEMENTS MORAUX D'UNE DÉFENSE DE LA VIE PRIVÉE

La défense morale d'un concept apporte son lot de défis. Difficile de procéder autrement qu'en présentant l'utilité fonctionnelle du concept si l'on veut dépasser la simple intuition morale de la supériorité d'une valeur donnée[235]. Pour cette raison, Ruth Gavison utilise une stratégie instrumentale pour justifier l'importance de la vie privée. Selon elle, la meilleure façon de comprendre la valeur d'un concept est d'examiner ses fonctions, soit de mettre en lumière comment le concept permet d'atteindre d'autres objectifs souhaités[236]. Ainsi, la force de la justification instrumentale dépendra d'une part de la désirabilité de ces autres objectifs et fonctions résultants du concept en question et d'autre part, de la force de la relation qu'il est possible entre le concept et lesdits objectifs[237]. Il s'agit donc de démontrer que les finalités liées à la vie privée sont importantes puisqu'elles sont effectivement liées à la vie privée. Pour ce faire, Gavison imagine un monde sans aucune vie privée dans lequel il y a un accès immédiat, complet et constant aux personnes : "[in] such a state, there would be no private thoughts, no private places, no private parts. Everything an individual did and thought would immediately become known to others"[238]. À partir de cette expérience de pensée, elle identifie les aspects de la vie humaine qui seraient rendus difficiles, voire impossibles sans vie privée. Elle distingue ce faisant sept fonctions de la vie privée essentielles aux individus et qui sont, à son sens, fortement souhaitables de protéger : la restriction de l'accès physique à soi, la promotion de la liberté d'action, une protection contre la censure et le ridicule, la promotion de la santé mentale, la promotion de l'autonomie, la promotion des relations humaines et la limitation de l'exhibition de soi.

Gavison le précise; elle n'a pas pour ambition de présenter chaque élément identifié de façon exhaustive et concluante et c'est pourquoi chacune des sept fonctions est présentée assez brièvement. C'est que son projet se veut sommaire et schématique des grands éléments en jeu dans la discussion sur la valeur morale de la privée[239]. Pour cette raison, son analyse fournit un excellent point de départ à partir duquel d'autres auteurs peuvent poursuivre la recherche. En effet, chacune

[235] Ruth Gavison dans Ferdinand David Schoeman, "Privacy and the limits of Law.", *Philosophical Dimensions of Privacy: An Anthology*, *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984): p.359-360.
[236] *Ibid.*, p.359.
[237] *Ibid.*
[238] *Ibid.*, p.360
[239] *Ibid.*, p.361

des fonctions de la vie privée identifiée par Gavison mérite de voir son analyse étayée, permettant ainsi d'augmenter la force de la justification morale. C'est justement ce qui est proposé dans cette section dans laquelle est approfondie une des fonctions identifiées par Gavison. L'argument fonctionnel présenté est celui qui démontre que la vie privée contribue à l'autonomie des personnes. Bien que toutes les fonctions de la vie privée identifiées par Gavison soient importantes, la capacité des personnes à cultiver leur autonomie apparaît particulièrement fondamentale, et d'ailleurs liée à plusieurs des autres fonctions de la vie privée telles que la promotion de la liberté d'action, et la protection contre la censure. De plus, cette fonction de la vie privée est particulièrement menacée dans le cyberespace comme cela sera démontré. Ainsi, en plus d'approfondir cet argument fonctionnel en faveur de la protection de la vie privée, cette section tâchera également de lier l'analyse aux enjeux particuliers du contexte numériques dépeints dans le second chapitre. Puis, il est démontré que la vie privée est non seulement liée à l'autonomie en ce qu'elle la promeut et la renforce, mais qu'elle constitue également un moyen défensif contre les menaces à l'égard de l'autonomie des personnes.

Avant de poursuivre avec l'analyse de l'autonomie comme valeur fonctionnelle du privé, il convient de traiter l'une difficulté de la stratégie instrumentale choisie pour ce projet. Cette stratégie a pour défaut de déplacer le problème de justification morale du concept sur ses finalités. En effet, la valeur du concept de vie privée que l'on désire défendre ici dépendra de la valeur accordée aux fonctions qu'on lui prête. Ainsi si l'on veut démontrer que la vie privée est importante parce qu'elle participe à l'autonomie des personnes, il faudrait également expliquer ensuite pourquoi l'autonomie des personnes est souhaitable, et ainsi de suite. Bien que l'importance de l'autonomie soit par endroit mise en valeur au cours de l'analyse, l'argument se concentrera plutôt sur la démonstration de la force du lien entre les deux concepts et sur l'exposition des manifestations de la détérioration de l'autonomie des personnes dans le monde numérique en raison du manque de vie privée. Ainsi, pour se sortir de cette impasse, on positionne la réflexion théorique dans une perspective libérale faisant la promotion d'une "society in which individuals can grow, maintain their mental health and autonomy, create and maintain human relations, and lead meaningful lives"[240]. Ainsi on tient pour acquis que les différentes vertus attribuées à la vie privée ci-dessous sont effectivement des finalités souhaitables dans une société libérale,

[240] *Ibid.*, p. 369.

démocratique et pluraliste dans laquelle est valorisée l'autonomie individuelle, la possibilité pour les personnes de mener le projet de vie qu'ils ont choisi pour eux-mêmes et la diversité.

L'autonomie, fonction de la vie privée

La « promotion de l'autonomie » est l'une des fonctions de la vie privée identifiée par Gavison. Cette dernière réfère plus spécifiquement à « l'autonomie morale », soit "the reflective and critical acceptance of social norms, with obedience based on an independent evaluation of their worth"[241]. Elle traite donc de ce qui permet aux individus de développer un jugement et des pratiques morales basés sur une capacité à réfléchir de façon critique par et pour soi-même. Aussi, avant de plonger dans l'analyse de l'argument de Gavison, il convient de discuter du concept d'autonomie de façon plus générale. En effet, alors que Gavison se concentre sur l'autonomie morale, la littérature présente différentes versions du concept d'autonomie. Il est généralement défini comme l'autodétermination de soi [242], et peut être associé à la moralité comme chez Gavison et chez Benn; "whose actions are governed by principles that are his own"[243]; à la volonté personnelle « d'être soi-même à l'origine de ses désirs »[244], ou encore à la liberté politique, soit de « pouvoir participer pour soi-même aux processus de prise de décision » d'un groupe ou d'une société[245]. Il s'agit en somme, pour un individu, d'être en mesure de penser, désirer, décider et faire pour soi-même sans subir d'influences ou de pressions extérieures dans l'exercice de ces différentes actions.

La définition ici proposée est, on le concède, très vaste. Comme Gerald Dworkin le souligne, le concept d'autonomie est en effet souvent utilisé de façon très large, parfois synonyme de liberté, parfois associé au libre arbitre, à la rationalité ou encore à la souveraineté. Le concept est également mis en relation, souligne Dworkin, avec des entités bien différentes : aux actions, aux personnes, à la volonté, aux désirs, aux principes des pensées, etc.[246]. Alors que le concept d'autonomie est de plus en plus populaire et profusément utilisé dans la philosophie politique moderne, Dworkin exhorte les théoriciens à préciser et définir la notion d'autonomie en fonction

[241] *Ibid.*, p.365.
[242] Nissenbaum, *op. cit*., p.81.
[243] *Ibid.*
[244] Sagnieres, *op. cit.*, p.9.
[245] *Ibid.,* p. 10.
[246] Gerald Dworkin, « Autonomy. A Companion to Contemporary Political Philosophy », *A Companion to Contemporary Political Philosophy*, 1 janvier 1988, p.443, https://doi.org/10.1002/9781405177245.

de leurs ambitions théoriques particulières [247]. Bien que l'approche analytique recommandée par Dworkin soit certainement essentielle pour la clarté de plusieurs travaux théoriques, une définition large est conservée pour cet exercice. Comme cela sera expliqué par la suite, les notions d'autonomie et de vie privée sont étroitement liées à plusieurs égards dans la littérature. Ainsi, notre démonstration ne se concentre pas uniquement sur un seul aspect ou une conception spécifique de l'autonomie, mais navigue plutôt entre les différents usages de l'autonomie utilisés par les auteurs traités, afin de mettre en lumière comment chacune de ces formes d'autonomie est liée à la vie privée. Après avoir développé l'argument de Gavison sur l'importance de la vie privée pour le maintien de l'autonomie des personnes à l'aide de l'analyse de Benn Stanley, notre argument est mis en contexte et illustré avec deux exemples du cyberespace.

La conception de l'autonomie de Gavison, comme cela a été mentionné, est basée sur l'autonomie morale. Sa perception est conforme à l'idéal kantien voulant que les principes moraux des personnes soient l'objet d'un choix rationnel[248]. Il y a dans l'autonomie de la raison, le principe suprême de la moralité, puisque sans cette autonomie, on se retrouve en proie à l'hétéronomie de l'arbitre, soit à être influencé par le monde qui nous entoure, sans pouvoir trouver un principe qui justifie rationnellement nos actions[249]. Gavison avance que sans vie privée, l'exercice de l'autonomie de la volonté devient difficile, voire impossible. Elle explique que même dans une société libérale ouverte et démocratique, il existe des pressions sociales qui découragent les individus à agir ou réfléchir en dehors des normes socialement imposées[250]. Ceci résonne notamment avec les thèses d'Alexis de Toqueville sur l'aphasie des peuples démocratiques[251], mais également avec les nombreuses études de psychologie sociale qui démontrent la tendance conformiste des personnes[252]. Or l'autonomie morale, telle que présentée par Gavison, exige la capacité à observer une distance critique vis-à-vis des autres (et de la majorité) afin de construire une réflexion indépendante. Gavison défend que la vie privée offre précisément cette distanciation nécessaire à l'exercice de l'autonomie morale :

> Privacy is needed to enable the individual to deliberate and establish his opinions. If public reaction seems likely to be unfavorable, privacy may permit an individual to

[247] *Ibid.*, p. 443.
[248] Emmanuel Kant, *Critique de la raison pratique* (Paris: Éditions Flammarions, 1788): p.130.
[249] *Ibid*., p.130
[250] Gavison, *op cit*, p.365.
[251] Alexis de Toqueville, *De la démocratie en Amérique, II* (Éditions Gallimard, 1961): p.345-361.
[252] Ophélie D., « Le conformisme: définition, explication et facteurs », *Publications Pimido*, 2014.

> express his judgments to a group of like-minded people. After a period of germination, such individuals may be more willing to declare their unpopular views in public. [253]

Ainsi, non seulement la vie privée serait-elle bénéfique au développement d'une pensée autonome, mais jouir de *privacy* serait une condition à la possibilité d'une pensée autonome. En effet, la vie privée offre la distance suffisante pour forger cette pensée, mais également l'espace et la liberté pour tester sa pensée, l'exercer et ainsi gagner la confiance nécessaire pour ensuite engager publiquement les idées qui en émergent. Cet argument selon lequel la vie privée est bénéfique, voire essentielle, au maintien de la capacité des personnes à réfléchir de façon indépendante et critique est également développé par Stanley Benn. Il explique que l'on agit différemment lorsque l'on se pense observé[254]. Il n'est pas nécessaire d'être dans une dynamique de surveillance comme dans le Panopticon pour que ce soit le cas. Lorsqu'une personne est en public, devant des collègues ou en compagnie d'amis, elle n'agit rarement avec la même liberté et insouciance que lorsqu'elle est seule avec elle-même ou bien avec une personne de laquelle elle ne craint aucun jugement. Benn précise que ce n'est pas toujours pas l'autorité d'un gouvernement ou d'une autre entité qui contraint le comportement, mais la simple pression exercée par les amis et voisins que l'on côtoie[255]. Ceci s'explique selon Benn parce que les personnes vivent selon des rôles bien définis qu'ils doivent remplir pour éviter de décevoir, la désapprobation ou encore le ridicule[256]. Il avance que la plupart des gens sont en mesure de se débarrasser de cette pression seulement dans des moments et espaces à l'abri de tout observateur externe :

> We need a sanctuary or retreat, in which we can drop the mask, desist for a while from projecting on the world the image we want to be accepted as ourselves, an image that may reflect the values of our peers rather than the realities of our natures. To remain sane, we need a closed environment, open only to those we trust, with whom we have an unspoken understanding that whatever is revealed goes no farther.[257]

Cet espace qu'offre la vie privée permet de créer une bulle, une distance suffisante pour cultiver la pensée critique, loin de l'opinion et du jugement d'autrui. On peut imaginer qu'un tel

---

[253] Gavison, *op cit*, p.365.
[254] Stanley Benn dans Ferdinand David Schoeman, "Privacy, Freedom and respect for persons.", *Philosophical Dimensions of Privacy: An Anthology*, *Philosophical Dimensions of Privacy* (Cambridge University Press, 1984) : p.241.
[255] *Ibid.*
[256] *Ibid.*
[257] *Ibid.*

espace demande avant tout d'être effectivement exempt de regards observateurs, mais puisse également permettre d'échanger avec des personnes de confiance comme le suggèrent Gavison et Benn. Tester ses idées avec des gens de confiance peut ainsi renforcer sa réflexion, contribuer à la forger ou la modifier aussi peut-être. L'autonomie en ce cas n'est pas affectée puisque, d'une part, la personne qui présente ses idées n'a pas peur de jugement de ces proches, et d'autre part, par ce que ces dernières n'ont pas pour objectif d'utiliser information connue sur leur ami pour le manipuler, le conditionner ou l'influencer de toute autre façon. Après avoir testé leurs idées dans de plus petits comités de confiance, les personnes gagnent ensuite en conviction et peuvent confronter l'opinion publique sans la crainte d'être pris pour des fous :

> The [autonomous] personal ideal is that of the independently minded individual, whose actions are governed by principles that are his own. This does not mean, of course, that he has concocted them out of nothing, but that he subjects his principles to critical review, rather than taking them over unexamined from his social environment. He is the man who resists social pressures to conform if he has grounds for uneasiness in doing the conformist thing.[258]

Marcel Becker compare deux approches normatives de la vie privée dans son article "Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy". Dans son analyse de l'approche individuelle, il dresse également un portrait du lien entre autonomie et vie privée, lien qu'il suggère être moins étroit que ce qu'entendent Benn et Gavison. Pour Becker, l'autonomie se résume au contrôle : "having control over one's own life"[259]. Ainsi, pour lui le lien entre autonomie et vie privée est clair dès lors que l'on considère cette dernière comme une façon de contrôler son environnement personnel : "[a] person who deliberately gains access to information that the other person wants to keep secret is violating the other person's autonomy through information control"[260]. Cependant, remarque Becker, une perte de vie privée n'implique pas nécessairement une perte d'autonomie. Il prend l'exemple d'une femme qui oublie régulièrement de fermer ses rideaux alors qu'elle se change, offrant une vue directe à son voisin. S'il y a effectivement perte de vie privée dans cet exemple, cette femme indique l'auteur : "still has the ability to control. At any moment, she could choose to close the curtains. Thus, privacy requires more than just autonomy"[261]. Ainsi, pour Becker, s'il y a effectivement un lien entre les

[258] *Ibid.*
[259] Becker, *op cit*, p.308.
[260] *Ibid.*
[261] *Ibid.,* p.309.

notions d'autonomie et de vie privée, ce lien n'est pas automatique. Il concède, proche en cela de Gerstain, que la vie privée est certainement un outil qui favorise le développement de l'autonomie au moyen de la délimitation d'un espace privée favorisant la construction pensée critique et indépendante[262]. Même si la vie privée peut contribuer positivement à l'autonomie des personnes, Becker reste catégorique : une perte de vie privée n'implique pas nécessairement une perte d'autonomie. Il est intéressant de constater que même en ayant dissocié, ou à tout le moins distancé, les deux concepts, Becker soutient que la perte de vie privée engendre généralement perte d'autonomie dans le contexte numérique[263]. Becker reconnaît qu'il existe une circonstance lors de laquelle la perte de vie privée engendre toujours une perte d'autonomie :

> A violation of privacy will result in autonomy being undermined only when at least one additional condition is met: the observing (privacy-violating) person is in one way or another influencing the other person (Taylor 2002). Such a violation of privacy can take various forms. For instance, the person involved might feel pressure to alter her behaviour just because she knows she is being observed. Or a person who is not aware of being observed is being manipulated.[264]

Donc, la violation de la vie privée, combinée à une influence de l'observateur sur l'observé, constitue alors toujours une perte d'autonomie selon Becker. On peut en effet concevoir que la manipulation, qui consiste à modifier les pensées ou les actions des personnes, corrompe la capacité à prendre des décisions indépendantes et donc l'autodétermination, ou le contrôle sur soi. On remarque que les deux exemples d'influence proposés dans l'extrait; la pression de se savoir observé et le fait d'être manipulé à son insu, sont malheureusement bien familiers. D'abord, la culture de surveillance exposée dans le chapitre précédent créé certainement une expérience panoptique pouvant influencer le comportement des personnes qui en sont conscientes. Ensuite, le profilage, le datamining et les *nudges*, qui ont pour objectif manifeste d'influencer les utilisateurs à leur insu, répondent également au critère d'influence de Becker. Ce dernier en conclut : "despite the fact that a loss of privacy does not necessarily involve a loss of autonomy, in the digital age when privacy is under threat, the independence of individual decisions is typically also compromised"[265].

[262] *Ibid.*
[263] *Ibid.*
[264] *Ibid.*
[265] *Ibid.*

Ceci illustre comment l'accès aux informations personnelles en ligne constitue un outil de manipulation, et met donc en péril l'autonomie des personnes. Dans ce contexte, la vie privée, et plus spécifiquement la protection des informations personnelles, constitue un moyen de défense contre les manipulations potentielles comme démontré ci-dessous. Mais on doit avant tout revenir sur la proposition de Becker, qui juge que la perte de vie privée ne constitue pas nécessairement une perte d'autonomie, puisqu'au moins un argument s'y oppose.

Selon Nissenbaum, si l'on considère que la vie privée implique à la fois les moyens de réguler l'accès à soi et l'autonomie comme l'autodétermination des personnes, pouvoir déterminer à qui donner accès ou non à ses informations (et donc à soi) est à la fois une pratique de vie privée et une pratique d'autonomie personnelle. Il faut bien comprendre qu'il ne s'agit pas ici d'une relation de cause à effet, mais bien de la nature même du concept d'autonomie : "privacy is to be understood as a form of autonomy: specifically, it is self-determination with respect to information about oneself"[266]. En ce sens, une personne dont la vie privée est brimée peut encore être autonome à certains égards : une femme peut en effet fermer le rideau de sa chambre à n'importe quel moment, mais elle perd une certaine forme d'autonomie dès lors que sa vie privée est brimée, ou plus précisément lorsqu'elle perd le contrôle sur ses informations. Si son voisin a observé son corps nu, et l'a photographiée à son insu, il est dès lors en possession d'informations privilégiées que cette femme n'entendait pas lui transmettre. En réalité, peu importe que la femme se sache ou non observée, ou que son voisin ait l'intention d'utiliser ces photos pour la faire chanter : elle a perdu son autonomie de décider devant qui elle désire ou non se dénuder. Autrement dit, elle a perdu le contrôle sur son image corporelle, elle ne contrôle plus l'accès des personnes à qui elle y donne accès, et perd donc une forme d'autodétermination sur elle-même et son propre corps. Suivant cette analyse, il convient que la perte de vie privée est toujours, en un sens au moins, une perte d'autonomie également. Ceci confirme la force du lien fonctionnel entre les deux concepts.

La vie privée : une arme défensive contre la manipulation

Il faut maintenant se poser la question; est-ce que la dégradation de l'autonomie par manque de vie privée a effectivement lieu dans le contexte numérique? Est-ce que le cyberespace permet le développement de personnes autonomes ou bien son manque de *privacy* a effectivement

[266] Nissenbaum, *op. cit*., p. 81.

pour effet de contraindre l'autonomie des personnes? Au moins deux indices pointent vers la seconde option : d'abord les utilisateurs des outils en ligne ressentent les effets de la surveillance et démontent des tendances à l'autocensure qui en résulte, et ensuite, les compagnies ont des pratiques de manipulation vis-à-vis de leurs usagers, dont les impacts sont déjà constatés.

D'abord, à savoir si les grandes compagnies de tech, parfois surnommées GAFAM, sont en constante surveillance de leurs utilisateurs, la réponse est oui[267]. Et les gens en sont de plus en plus conscients comme le démontrent les sondages[268]. Il est donc fort probable que les gens commencent à changer leur comportement plus cette conscience sera grande. Est-ce qu'une jeune femme sera à l'aise d'aller acheter les suppléments recommandés par son médecin si elle craint que la compagnie où elle compte faire ses achats envoie de la publicité ciblée de grossesse chez ses parents? Est-ce qu'une personne sera se sentira libre d'afficher son orientation sexuelle en ligne si elle a peur que cette information soit divulguée à son insu à sa famille ou des groupes haineux[269]? Est-ce qu'une famille se sentira suffisamment en sécurité pour tenir une conversation sensible ou un débat polémique dans son propre salon sans risquer qu'ils soient enregistrés par leurs objets connectés et partagés dans leur réseau professionnel[270]? Ces exemples sont en l'occurrence tous tirés de faits véritables.

Selon Harcourt: "[this] omnipresent knowledge deprives us of a secure space of our own, a place to feel safe, protected"[271]. Des recherches suggèrent que la visibilité en ligne et l'exposition constante à la transparence sur les réseaux sociaux ont effectivement des effets négatifs sur la disposition et la propension des gens à partager leurs opinions publiquement[272]. Ceci serait particulièrement vrai lorsque les personnes pensent avoir une opinion minoritaire[273]. Une étude montre les résultats de cette « spirale du silence »[274]. Le sondage effectué sur 1800 personnes

[267] Harcourt, *op. cit.,* p.220; Véliz, *op. cit*., p.86.
[268] Statistique Canada, « Canadian's assessments of social media in their lives ».
[269] Josh Halliday, « Facebook users unwittingly revealing intimate secrets, study finds | Facebook | The Guardian », *The Gardian*, mars 2013, https://www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets.
[270] Tom Warren, « Amazon explains how Alexa recorded a private conversation and sent it to another user - The Verge », *The Verge*, mai 2018, https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation.
[271] Harcourt, *op cit*, p.221
[272] *Ibid.*, p.219
[273] *Ibid.*
[274] Matteo Cinelli et al., « The echo chamber effect on social media », *Proceedings of the National Academy of Sciences* 118, nº 9 (mars 2021), https://doi.org/10.1073/PNAS.2023301118.

révèle que les utilisateurs de Facebook sont plus disposés à partager leur point de vue s'ils pensent que les personnes qui les suivent sur la plateforme sont d'accord avec eux[275]. Il apparaît également que les répondants qui utilisent des réseaux sociaux comme Facebook et Twitter étaient au moins deux fois moins enclins que les autres à partager leurs opinions même dans des contextes en personne, comme avec des amis dans un restaurant[276]. Il semble donc que les utilisateurs des réseaux sociaux internalisent la culture de transparence dans laquelle ils se sentent toujours observés (et jugés), jusqu'à en subir les effets dans leur vie quotidienne et dans les espaces qui devraient autrement être suffisamment privés pour permettre le développement de réflexions critiques.

Enfin, les grandes compagnies de tech et leurs algorithmes sont déjà réputés pour leurs pratiques visant à influencer leurs utilisateurs. L'influence est parfois ciblée et dirigée par des intentions précises. On pense bien sûr au scandale de Cambridge Analytica, à l'occasion duquel les données de 87 millions d'utilisateurs Facebook ont été utilisées afin d'identifier leurs convictions politiques et caractéristiques psychologiques afin de cibler des messages et publicités politiques dans le but d'influencer leur vote[277]. Ainsi, en fonction des enjeux particuliers ayant été identifiés comme importants pour une personne dont le vote était incertain, cette dernière pouvait recevoir des informations visant à renforcer une certaine position politique, incluant de fausses informations[278]. Certes, la propagande n'est pas un phénomène nouveau. Mais Véliz remarque qu'elle était autrefois publique et accessible à tous : "[what] is particularly unhealthy about personalized propaganda is that it contributes to polarization through showing each person different and potentially [false] information, and it takes advantage of people's personality traits to be more effective in influencing them"[279]. La propagande individuelle pose un problème bien plus grand pour l'autonomie morale puisque cela "fractures the public sphere into atomic individual spheres"[280], et rend d'autant plus difficile pour chaque personne de trouver une distance critique vis-à-vis des informations sur-mesure qu'il ou elle reçoit. Sans compter le problème majeur que le pouvoir d'influencer le résultat d'une élection par ce genre de manipulation engendre

[275]Keith Hampton, Lee Rainie, et Weixu Lu, « Social Media and the 'Spiral of Silence' », Pew Research Center, 2014. p.3 https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/.
[276] *Ibid*., p.4
[277] ur Rehman, *op. cit*.
[278] Carissa Véliz, « The Internet and Privacy », *Ethics and the Contemporary World*, 2019. p.3
[279] *Ibid.*
[280] *Ibid.*

pour toute démocratie, il faut aussi constater la problématique au niveau individuel : ce type manipulation subtil et orchestré, rendu possible par l'accès aux données personnelles pose un réel problème en ce qui a trait à la capacité des personnes à développer une pensée autonome.

Maintenant, comment protéger son autonomie morale, politique et de libre arbitre? Pour Véliz, la réponse réside dans la protection de la vie privée. Pour elle, l'autonomie est le fait d'avoir le pouvoir sur sa propre vie [281]. Elle défend que les informations personnelles, lorsqu'accessibles à autrui, leur donnent du pouvoir sur soi. En effet, elle explique comment la connaissance confère du pouvoir : "the more someone knows about us, the more they can anticipate our every move, as well as influence us"[282]. Les informations personnelles, celles que la plupart des gens préfèrent ne pas partager avec tout le monde[283], peuvent être utilisées par les autres de façons bien différentes explique Véliz. Par exemple, lorsque ses informations sont partagées avec des personnes de confiance qui ont son bien-être à cœur; amis, famille ou être aimé, une personne peut en tirer beaucoup de bonheur puisque ces personnes utiliseront généralement ce qu'elles savent à bon escient[284]. L'intimité partagée avec ses proches pourrait au contraire participer à renforcer l'autonomie. Cependant, les informations personnelles peuvent également être utilisées pour prédire les comportements, tenter de les influencer ou encore prendre des décisions au sujet d'une personne, comme il a été présenté dans le chapitre deux. Partager ses secrets, ses peurs et ses désirs avec quelqu'un, donne à cette personne du pouvoir sur soi. S'ouvrir à l'autre, c'est également ouvrir la porte à être blessé, trompé ou manipulé. Avoir de l'information sur une personne permet en effet d'interférer plus facilement dans sa vie[285]. C'est probablement pourquoi les publicités ciblées, les fraudes personnalisées et les systèmes de recommandations basés sur les préférences fonctionnent si bien. Pour cette raison, Véliz affirme que la vie privée est importante parce que le manque de vie privée donne à autrui du pouvoir sur sa personne, et donc restreint son autonomie : "[through] protecting our privacy, we prevent others from being empowered with

[281] Véliz, « Privacy is Power », *op. cit*., p.84.
[282] *Ibid*., p.61.
[283] « Privacy is like the key that unlocks the aspects of yourself that are most intimate and personal, that most make you *you*. Your sexual history and fantasies. Your past, present, and possible future diseases. Your fears, your losses, your failures. The worst things you have ever done, said, and thought. Your inadequacies, your mistakes, your traumas. The moment in which you have felt most ashamed. That family relation you wish you didn't have. Your most drunken night. » Dans Véliz, « Privacy is Power », *op. cit*., p.55-56.
[284] Véliz, « Privacy is Power », *op. cit*., p.56.
[285] *Ibid.*, p.84.

knowledge about us that can be used against our interests"[286]. En ce sens, la vie privée est peut-être, dans le cyber espace du moins, la meilleure façon de protéger son autonomie.

Pour conclure sur le lien entre l'autonomie et la vie privée, on doit répondre à la critique selon laquelle même dans des sociétés très totalitaires, avec peu de respect pour la vie privée, il y a toujours eu des individus qui réussissent à garder une certaine autonomie [287]. Ce contre-argument avance que même sans vie privée, il est possible pour certaines personnes de conserver une forme d'autonomie; sa capacité de jugement et de réflexion critique, soit son autonomie morale. La réponse de Gavison à ce propos semble suffisante pour maintenir une position en faveur de la protection de la vie privée : "[even] if we grant that privacy may not be a necessary condition for autonomy for all, however, it is enough to justify it as a value that most people may require it. We are not all giants, and societies should enable all, not only the exceptional, to seek moral autonomy"[288]. En effet, dans le contexte d'une société libre et démocratique, qui entend offrir la possibilité aux personnes se développer, de mener les projets de vie qu'ils ont choisis et de faire des choix pour eux-mêmes, il apparaît évident que d'offrir la possibilité de maintenir un niveau de vie privée suffisant pour entretenir leur autonomie est essentiel. On peut invoquer ici le conséquentialisme kantien qui exige le respect des personnes en tant que fins en soi ainsi que l'autonomie de la raison comme principe suprême de la moralité[289].

Pour assurer que les personnes puissent développer leur autonomie morale, elles doivent pouvoir être en mesure de maintenir un certain niveau de vie privée. Si l'on met en péril l'autonomie morale des personnes pour des fins commerciales, ou politiques, on considère ces dernières comme moyen non comme fins. En fait, même si cela n'est pas l'objet de ce chapitre, on peut penser que les seules instances lors desquelles il serait justifié de piler sur la vie privée des personnes sont lorsqu'elles sont conçues comme des fins en soi. Lorsqu'une personne va chez le médecin, elle renonce à une certaine forme de vie privée, dévoilant au professionnel des informations personnelles, parce que dans cette situation l'objectif est de lui prodiguer les meilleurs soins de santé possible : elle est la fin en soi. Dans cette situation, il est également probable que la diminution de sa privée est tellement minime et contrôlée que la personne n'en

[286] *Ibid.*, p.56.
[287] Gavison, *op. cit.*
[288] *Ibid.*, p.365.
[289] Kant, *op. cit*.

subisse pas de conséquence sur son autonomie. Cette même analyse peut être déployée à plus grande échelle lorsque la société désire par exemple mettre en place des initiatives comme l'application de traçage des déplacements pendant la pandémie. Il faut s'assurer que les personnes sont effectivement traitées comme des fins en soi dans le déploiement de l'initiative, et que l'atteinte à leur vie privée est suffisamment encadrée pour ne pas mettre en danger leur autonomie.

Voici donc qui montre comment la vie privée est liée à l'autonomie : elle est à la fois un outil permettant de développer l'autonomie des personnes, mais constitue également un moyen défensif contre les différentes menaces qui mettent en péril cette même autonomie dans le monde numérique. Aussi dans ce contexte, on se doit d'assurer que la possibilité de maintenir des processus de vie privée adéquats, notamment pour maintenir l'autonomie des personnes. C'est sur la base de cet argument moral qu'il est défendu que la vie privée devrait être au centre des préoccupations en ce qui a trait à la gestion du cyberespace, que ce soit par les gouvernements, la société civile ou d'autres entités.

LA PROTECTION DE LA VIE PRIVÉE EST UN ENJEU DE SOCIÉTÉ

Ce qui a été soulevé jusqu'à présent dans ce mémoire est que la vie privée, conçue comme les processus permettant de réguler l'accès à soi, est importante parce qu'elle permet de maintenir l'autonomie des personnes, et deuxièmement qu'il n'y a peu, ou pas de vie privée en ligne. Cette dernière section entend d'abord tabler sur la question du consentement à l'utilisation des données afin de rejeter l'argument selon laquelle les personnes dans le monde numérique renoncent en fait à protéger leur vie privée. Ensuite, on revient sur la définition de la vie privée élaborée dans le premier chapitre, afin de démonter comment la protection de la vie privée s'agit non seulement d'un enjeu individuel de protection d'autonomie, mais également et surtout, un enjeu collectif qui doit être conçu comme un projet de société. Ce faisant, quelques nuances sur les limites souhaitables de la vie privée seront également apportées.

Vers une culture de la privacy et un environnement sécuritaire dans le monde numérique

Devant le manque de vie privée qui caractérise le cyberespace, et considérant la valeur de la vie privée qui doit être protégée, on peut maintenant poser la question : comment faire? Dans le premier chapitre, une définition processuelle de la vie privée a été développée à la suite d'Irwin Altman. La vie privée est ainsi considérée comme les moyens ou processus de *privacy* qu'une

personne ou un groupe emploie pour se rendre plus ou moins accessible aux autres. Il existe d'après Altman, rappelons-le, quatre types de processus par lesquels une personne peut assurer sa vie privée ; des mécanismes verbaux, comportementaux, environnementaux, et culturels[290]. On peut se demander si chacun de ces types de stratégie de *privacy* trouve son équivalent dans le monde numérique. Si les mécanismes verbaux sont dans le monde naturel le fait d'adapter ses propos ou le ton de sa voix en fonction de son audience et du lieu dans lequel on se trouve afin de donner plus ou moins d'information, alors ce processus pourrait se traduire dans le monde par le type d'information que les personnes choisissent ou non de partager. Ce processus, qui pourrait se traduire par un processus de contrôle de l'information, inclurait par exemple de publier moins de contenu en ligne, de donner le moins d'informations personnelles possible aux différentes plateformes utilisées, et ainsi de suite. On image ensuite que la seconde catégorie de mécanisme, les comportementaux, pourrait inclure toutes les « meilleures pratiques » de sécurité numérique telles qu'utiliser un navigateur de recherche sécurisé, vérifier et changer si possible les paramètres de confidentialité par défaut des outils utilisés, ne pas utiliser des outils de stockages d'information nuagiques pour conserver des informations personnelles, intégrer des outils permettant d'éviter le traçage, choisir les applications de messagerie avec des chiffrements de bout en bout (*end-to-end encryption*), toujours naviguer à partir de réseaux wi-fi privés et sécurisés, etc.[291].

On remarque que ces deux premiers types de processus sont du ressort des individus. Il revient aux personnes de mettre en place ces stratégies afin de réguler l'accès à soi. Aussi, on peut se demander, avec raison, si les personnes n'ont pas une part de responsabilité dans la régulation de l'accès à leurs informations en ligne. La vie privée, à l'aide des deux processus décrits ci-dessus, est quelque chose qui s'entretient et nécessite une certaine proactivité des personnes pour la maintenir. Les gens ne devraient-ils pas se conscientiser face aux enjeux de vie privée, et s'ils désirent effectivement préserver leur vie privée, que ça soit pour entretenir leur autonomie ou d'autres raisons qui leur sont propres? Et alors, ne pourraient-ils pas faire des choix en conséquence, en adoptant par exemple certaines des stratégies mentionnées ci-haut? C'est effectivement la position des économistes néoclassiques qui défendent que ce soit du ressort des utilisateurs de choisir en fonction de leurs priorités et objectifs[292]. Le maintien d'une vie privée en

[290] Altman, *op. cit*., p.33-42.
[291] Quelques-uns des trucs et astuces recommandés dans une revue technologique : Alex Perekalin, « Ten tips to improve your Internet privacy | Kaspersky official blog », *Kaspersky Daily*, avril 2019.
[292] Pasquale, *op. cit*., p.80

lignes par des choix intelligents que proposent les économistes néoclassiques est une fausse solution, parce que ce choix est dans les faits inexistant.

Effectivement, les personnes ont sans aucun doute un certain rôle à jouer au niveau individuel sur le maintien de leur vie privée, et dire le contraire serait en opposition directe avec le principe d'autonomie prôné plus tôt. Or, force est de constater que le maintien de la vie privée en ligne n'est pas réellement accessible pour toutes les personnes. Les structures en place dans le cyber contreviennent à la mise en place de stratégies de protection des données, et favorisent un accès toujours plus grand aux personnes à des fins économiques, politiques ou de sécurité. Les moyens de *privacy* à disposition sont tantôt inefficaces, tantôt inexistants. En effet, il a été démontré à plusieurs reprises que plusieurs des outils de protection recommandés par les journalistes des revues de technologie ont été compromis, déjoués ou ne fonctionnent que partiellement[293]. Aussi, les moyens de vérifier l'efficacité réelle de ces stratégies de *privacy* sont quasiment inexistants pour toute personne n'ayant pas une connaissance approfondie des technologies informatiques. Ainsi, la meilleure façon de protéger sa vie privée reste pour la plupart des gens de renoncer à utiliser ces outils numériques. Cette solution, il l'a été abordé plus tôt, en plus d'être assez extrême considérant les avantages considérables qu'apportent ces outils, est de façon pratiquement impossible à mettre place en raison des pressions économiques et sociétales. Bref, s'il est possible de maintenir un certain degré de vie privée en ligne, la responsabilité de mettre les processus nécessaires pour y arriver revient entièrement aux personnes, puisque les processus environnementaux (*privacy by design*) sont pratiquement inexistants. Et s'il est en théorie possible pour les personnes de mettre en place des processus de *privacy*, le coût social de ces processus est tellement élevé qu'il rend pratiquement impossible pour la personne moyenne de le mettre en place, à moins d'avoir un très fort degré de littéracie numérique et le temps de les mettre en place, ou encore des moyens financiers assez élevés pour que d'autres le fassent. Les stratégies de *privacy* à disposition demandent un effort tellement considérable que les personnes renoncent finalement à mettre en place ces stratégies, dont l'efficacité est de toute façon questionnable.

Dans les lieux publics, lorsque nécessaire, on peut généralement compter sur les infrastructures en place pour assurer sa la protection de sa vie privée. Lorsque l'on va à l'hôpital,

[293] *Ibid*., p.54

on peut compter sur des salles de consultation fermées et la responsabilité professionnelle du docteur pour protéger la confidentialité de ses informations. Les cabines téléphoniques, les toilettes publiques, les salles d'essayage, les isoloirs aux bureaux de vote, tant de structures accessibles publiquement parce que la société considère important de préserver la *privacy* des personnes dans les espaces publics également. Aussi pour garantir aux personnes une possibilité réelle de maintenir une protection adéquate de leur vie privée en ligne, des processus de nature environnementaux et culturels doivent être développés, qu'il s'agisse d'infrastructures numériques mieux sécurisées, de mettre en place des normes minimales de *privacy* en ce qui concerne le design des technologies et applications, de l'imposition de pratiques responsables de collecte de données par les grandes entreprises, soit de ne collecter que les données nécessaires, et de supprimer ces dernières une fois leur utilité remplie. En prenant pour pierre d'assise une théorie de la justice admettant des libertés fondamentales aux personnes, notamment la possibilité de se développer de façon autonome, et offrant un accès non seulement théorique, mais bel et effectif à ces libertés, la conclusion à laquelle porte le présent travail est que la protection de la vie privée est un enjeu d'intérêt public dont le déploiement doit être pris en charge par les institutions publiques.

CONCLUSION

Dans ce mémoire, nous nous sommes penchés sur un sujet d'actualité : celui de l'impact des nouvelles technologies de l'information sur la vie privée, explorant les considérations philosophiques impliquées dans ce contexte. La valeur de la vie privée semblant avoir été remise en question par des pratiques de partage incessant de l'information, nous avons exploré la place de cette dernière dans le cyberespace. Il nous a d'abord fallu nous doter d'une définition pour le concept de vie privée, ce dernier étant peu consensuel dans la littérature. La définition retenue est une conception processuelle de la vie privée, c'est-à-dire que celle-ci réfère aux processus de *privacy* qui servent à limiter l'accès à soi, qu'ils soient mis en place par les individus ou présents dans l'environnement. Cette définition a avant tout l'avantage d'être neutre. Étant exempte de considérations normatives, elle nous a permis de circonscrire le concept de vie privée de manière objective, sans égard à ce qui devrait être ou non privé. Notre définition a également la qualité d'être suffisamment générale pour traiter de la vie privée dans plusieurs contextes, dont celui numérique dans lequel la nature de ce qui est à protéger par les différents processus de *privacy* est largement informationnelle : les données.

Ainsi dotés d'une définition claire et précise de ce qui est entendu par vie privée nous nous sommes alors intéressés au contexte particulier qui motive notre question de recherche, à savoir : qu'en est-il de la vie privée à l'ère des données massives? Ce chapitre nous a permis d'identifier les spécificités propres aux nouvelles technologies qui posent de nouveaux défis à la protection de la vie privée. Il nous était en effet essentiel de comprendre les caractéristiques particulières de ce contexte puisque les nouvelles technologies au cœur de celui-ci ont transformé les enjeux de vie privée. En effet, la numérisation des données et les nouvelles capacités de traitement de l'information offrent un accès direct aux personnes en plus de permettre l'accumulation d'information dans le temps en raison de la pérennité des données numériques ainsi que des capacités de stockages augmentées. Les algorithmes offrent à leur tour des possibilités sans précédent maximisant le potentiel informatif des données, et donc d'accès aux personnes. Ensuite, ce chapitre a également mis en lumière des dynamiques et structures qui limitent la mise en place

de processus de *privacy* dans le cyberespace. En effet, il n'y a pas seulement la nature des nouvelles technologies de l'information qui pose problème, mais également des dynamiques structurelles en place dans le cyberespace comme la culture de surveillance et le régime de visibilité. Bref, ce second chapitre a mis la table sur les enjeux et le contexte particulier dans lequel les questions de vie privée se posent à l'heure actuelle, démontrant qu'il n'y a pas ou peu de processus de *privacy* en ligne, et donc pas de vie privée numérique.

Enfin, le dernier chapitre confère son ton normatif au mémoire, défendant l'importance de la vie privée. Nous y avons d'abord abordé certaines des discussions qui contribuent à remettre en question la valeur de la vie privée, soit le mythe du « *privacy paradox* » et la question de la magie morale du consentement. Alors que le premier sous-entend à tort que la vie privée est une valeur dépassée, ou du moins délaissée, le second offre une solution viciée aux enjeux de vie privée numérique, minimisant par ailleurs ces derniers. Nous avons donc déconstruit ces deux arguments, démontrant qu'il s'agit d'un faux paradoxe ainsi que d'une fausse bonne idée qui ne doivent donc pas remettre en question l'importance des enjeux de vie privée et la valeur de cette dernière. Le chapitre se conclut sur un argument moral qui démontre l'importance de protéger la vie privée numérique dévoilant les liens profonds entre l'autonomie et la vie privée, puis exposant la fonction défensive de cette dernière.

Ceci nous amène enfin aux conclusions de ce mémoire. Qu'en est-il donc de la vie privée dans le contexte du *Big Data*? Au terme de notre analyse, il apparaît que la vie privée est affectée par le contexte numérique, en ce sens que les processus de *privacy* numériques sont insuffisants, voire inexistants. Il est également mis en évidence que la vie privée est une valeur essentielle pour le bien-être des individus et des sociétés et donc que les enjeux exposés dans ce mémoire doivent être adressés.

Dans ce contexte, l'apport de ce mémoire est certes petit, mais important. Il offre d'une part une présentation des différents éléments qui prennent part aux problèmes de vie privée numérique auxquels les sociétés sont confrontées. Il présente également plusieurs outils théoriques qui peuvent contribuer à faire avancer la littérature sur la question, comme une définition de la vie privée et son intégration au modèle informationnel de Floridi. Il reste toutefois de nombreuses questions à éplucher en lien avec la vie privée numérique et ce mémoire n'en fait qu'une esquisse. Si le consentement n'est pas une solution acceptable pour réguler l'accès aux données, il faut par

exemple réfléchir à quelle matrice morale peut servir à encadrer l'économie des données. Il faudrait probablement également questionner la moralité même de cette économie des données. Comment concilier le dilemme moral qui oppose les bienfaits de l'utilisation des données et les risques pour la vie privée qui en découlent? Telle sera possiblement la plus grande contribution de ce mémoire : de motiver d'autres travaux sur la question. C'est du moins la note sur laquelle nous désirons conclure. L'apport des philosophes dans les débats publics sur les enjeux en lien avec les nouvelles technologies est essentiel. Ce mémoire est donc une invitation à poursuivre le travail théorique et pratique nécessaire pour guider les débats éthiques actuels et futurs.

BIBLIOGRAPHIE

Abiteboul, Serge. « Sciences de données. De la logique du premier ordre à la Toile ». Présenté à leçon inaugurale à la chaire Informatique et sciences numériques du Collège de France, 8 mars 2012.

Altman, Irwin. *The Environment and Social Behavior*. Brooks/Cole Publishing Compagny, 1975.

Bacach-Beauvallet, Maya, Yann Bonnet, Olivier Henrard, Pascale Idoux, et Winston Maxwell. « Le rôle des données et des algorithmes dans l'accès aux contenus ». Les mutations de la mise à disposition de contenus audiovisuels à l'ère du numérique : conséquences et enjeux. CSA Lab, 2017.

Basdevant, Adrien, et Jean-Pierre Mignard. *L'empire des données: essai sur la société, les algorithmes et la loi*. Don Quichotte éditions, 2018.

Bawden, David, et Lyn Robinson. « "The dearest of our possessions": Applying Floridi's information privacy concept in models of information behavior and information literacy ». *Journal of the Association for Information Science and Technology* 71, nº 9 (2020): 1030-43. https://doi.org/10.1002/asi.24367.

Becker, Marcel. « Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy ». *Ethics and Information Technology* 21 (juillet 2019): 307-17. https://doi.org/10.1007/s10676-019-09508-z.

Beckouche, Pierre. « La révolution numérique est-elle un tournant anthropologique ? », Le Débat, 193, nº 1 (2017): 153-66.

Bietti, Elettra. « The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond ». *Stanford University Aegis Paper Series*, nº 2001 (2020).

boyd, danah, et Alice Marwick. « Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies ». *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, septembre 2011, 1-29. https://doi.org/10.31219/osf.io/2gec4.

Brown, Rodney. « Defition : Petabyt ». TechTarget, s. d. https://searchstorage.techtarget.com/definition/petabyte.

Bucher, Taina. « Want to be on the top? Algorithmic power and the threat of invisibility on Facebook ». *New Media & Society* 14, nº 7 (avril 2012): 1164-80. https://doi.org/10.1177/1461444812440159.

Burns, Anne-Marie. « Compte rendu de [MARTIN MICHAUD, Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute, 1996] ». *Les Cahiers de droit* 38, nº 1 (1997): 231-39.

Casilli, Antonio. « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée ». Etude annuelle 2014 du Conseil d'Etat. Le numérique et les droits fondamentaux. La Documentation Française, 2014. http://cvpip.wp.mines-telecom.

Cinelli, Matteo, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi, et Michele Starnini. « The echo chamber effect on social media ». *Proceedings of the*

National Academy of Sciences 118, nº 9 (mars 2021). https://doi.org/10.1073/PNAS.2023301118.

Clark, Tom C., et Alan F. Westin. « Privacy and Freedom ». *California Law Review* 56, nº 3 (1968): 911-911. https://doi.org/10.2307/3479272.

Commissariat à la protection de la vie privée du Canada. « Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019 », s. d. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/#fig03.

Craig, Terence, Mary E. Ludloff, et Jennifer Geetter. *Privacy and big data*. *Computer*. O'Reilly Media, 2011. https://doi.org/10.1109/MC.2014.161.

D., Ophélie. « Le conformisme: définition, explication et facteurs ». *Publications Pimido*, 2014.

Decew, Judit. « Privacy ». In *Stanford Encyclopedia of Philosophy*, 2018. https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Decew, Judith Wagner. « The Scope of Privacy in Law and Ethics ». *Law and Philosophy*, Springer, 5, nº 2 (1986): 145-73.

Dilhac, Marc-Antoine, et Christophe Abrassart. « Déclaration de Montréal pour un développement responsable de l'intelligence artificielle ». Montréal: Université de Montréal, 2018.

Dworkin, Gerald. « Autonomy. A Companion to Contemporary Political Philosophy ». *A Companion to Contemporary Political Philosophy*, 1 janvier 1988, 443-51. https://doi.org/10.1002/9781405177245.CH18.

Floridi, Luciano. « Four challenges for a theory of informational privacy ». *Ethics and Information Technology* 8, nº 3 (2006): 109-19. https://doi.org/10.1007/s10676-006-9121-3.

Floridi, Luciano. *The fourth revolution: how the infosphere is reshaping human reality*. Oxford University Press, 2014.

Floridi, Luciano. « The ontological interpretation of informational privacy ». *Ethics and Information Technology*, 2005. https://doi.org/10.1007/s10676-006-0001-7.

Foucault, Michel. *Surveiller et punir : naissance de la prison*. Éditions G., 1993.

Froment, Dominique. « Votre épicier en sait peut-être plus sur vous que votre conjoint ». *Les Affaires*, s. d. https://www.lesaffaires.com/dossier/creer-l-avenir-maintenant/votre-epicier-en-sait-peut-etre-plus-sur-vous-que-votre-conjoint/541930.

Golladay, Katelyn, et Kristy Holtfreter. « The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes ». *Victims and Offenders* 12, nº 5 (3 septembre 2017): 741-60. https://doi.org/10.1080/15564886.2016.1177766.

Halliday, Josh. « Facebook users unwittingly revealing intimate secrets, study finds | Facebook | The Guardian ». *The Gardian*, mars 2013. https://www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets.

Hampton, Keith, Lee Rainie, et Weixu Lu. « Social Media and the 'Spiral of Silence' », PEW RESEARCH CENTER, 2014. https://www.pewresearch.org/internet/2014/08/26/social-media-and-the-spiral-of-silence/.

Harcourt, Bernard E. *Exposed*. Édité par Harvard University Press, 2015.

Henschke, Adam, et On Privacy. « On Privacy ». In *Ethics in an Age of Surveillance*, 28-55. Cambridge: Cambridge University Press, 2014. https://doi.org/10.1017/9781316417249.002.

Hoven, Jeroen van den, Martijn Warnier, et Pieters Wolter. « Privacy and Information Technology ». In *The Stanford Encyclopedia of Philosophy*. Summer 2020 Edition, s. d. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.

Igo, Sarah E. *The Known Citizen : A History of Privacy in Modern America*. Harvard University Press, 2018.

Ingram, David. « Facebook fuels broad privacy debate by tracking non-users ». *Reuters*, 2018. https://www.reuters.com/article/us-facebook-privacy-tracking-idUSKBN1HM0DR.

Johani, Mashael A L. « Personal Information Disclosure and Privacy in Social Networking Sites ». Auckland University of Technology, 2016.

Kant, Emmanuel. *Critique de la raison pratique*. Paris: Éditions Flammarions, 1788.

Kleinig, John. « The Nature of Consent ». In *The Ethics of Consent : Theory and Practice*, édité par Franlklin G Miller et Alan Wertheimer, Oxford University Press., 91-118, 2010. https://doi.org/10.1080/00455091.1982.10715825.

Kramer, Irwin R. « The Birth of Privacy Law: A Century Since Warren and Brandeis ». *Catholic University Law Review Cath. U. L. Rev* 39, nº 3 (1990). http://scholarship.law.edu/lawreview%0Ahttp://scholarship.law.edu/lawreview/vol39/iss3/3.

Kudina, Olya, et Melis Baş. « "The end of privacy as we know it": Reconsidering public space in the age of Google Glass ». In *Surveillance, Privacy and Public Space*, 1st Edition., 119-40. Routledge, 2018.

Latzko-Toth, Guillaume, et Madeleine Pastinelli. « Par-delà la dichotomie public/privé : la mise en visibilité des pratiques numériques et ses enjeux éthiques ». *Tic & société [Online]* 7, nº 2 (2014). https://doi.org/10.4000/ticetsociete.1591.

Lee, Kai-Fu. *AI Superpowers: China, Silicon Valley, and the New World Order*. Houghton Mifflin Harcourt, 2018. https://doi.org/10.1007/s11366-020-09674-8.

Lessig, Lawrence. *C o d e*. Vol. 346. Basic Book, 2006.

Lyon, David. « Surveillance culture: Engagement, exposure, and ethics in digital modernity ». *International Journal of Communication* 11, nº February (2017): 824-42.

Marx, Gary T. « Humpty Dumpty Was Wrong - Consistency in Meaning Matters: Some Definitions of Privacy, Publicity, Secrecy, and Other Family Members ». *Secrecy and Society* 1, nº 1 (2016).

Montag, Christian, Bernd Lachmann, Marc Herrlich, et Katharina Zweig. « Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories ». *International Journal of Environmental Research and Public Health* 16, nº 14 (2 juillet 2019). https://doi.org/10.3390/IJERPH16142612.

Moore, Adam. « Defining Privacy ». *Journal of Social Philosophy* 39, nº 3 (septembre 2008): 411-28. https://doi.org/10.1111/j.1467-9833.2008.00433.x.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Standford University Press, 2010.

Nycyk, Michael. « From data serfdom to data ownership: An alternative futures view of personal data as property rights ». *Journal of Futures Studies* 24, nº 4 (2020): 25-34. https://doi.org/10.6531/JFS.202006_24(4).0003.

Office québécois de la langue française (OQLF). « algorithme prédictif ». In *Grand dictionnaire terminologique*, s. d. http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26543863.

Office québécois de la langue française (OQLF). « apprentissage automatique ». In *Grand dictionnaire terminologique*, s. d. http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8395061.

O'Neil, Cathy. *Weapons of Math Destruction: how big data increases inequality and threatens democracy*. Kindle Edi., 2016.

Paasonen, Susanna. « Affect, data, manipulation and price in social media ». *Distinktion* 19, nº 2 (2018): 214-29. https://doi.org/10.1080/1600910X.2018.1475289.

Parent, W A. « Privacy, Morality, and the Law ». *Philosophy & Public Affairs* 12, nº 4 (1983): 269-88.

Pasquale, Frank. *The Black Box Society : The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

Perekalin, Alex. « Ten tips to improve your Internet privacy | Kaspersky official blog ». *Kaspersky Daily*, avril 2019.

Powers, Madison. « A Cognitive Access Definition of Privacy ». *Law and Philosophy* 15, nº 4 (1996): 369-86.

Reiman, Jeffrey H. « Privacy, Intimacy, and Personhood ». *Philosophy & Public Affairs* 6, nº 1 (1976): 26-44.

Robertson, Viktoria H.S.E. « 'Excessive data collection: Privacy considerations and abuse of dominance in the era of big data », Common Market Law Review, nº Issue 1 (2020): 161-90.

Rochelandet, Fabrice. « I Définition : vie privée et données personnelles ». In *Économie des données personnelles et de la vie privée*, La Découve., 128-128. Paris, 2010. https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652.htm.

Rochelandet, Fabrice. « II Quelles justifications à la vie privée ». In *Économie des données personnelles et de la vie privée*, La Découve., 128-128. Paris, 2010.

Rona-Tas, Akos. « Predicting the Future: Art and Algorithms ». *Socio-Economic Review* 18, nº 3 (2020): 893-911. https://doi.org/10.1093/ser/mwaa040.

Rouvroy, Antoinette. « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data ». *Le numérique et les droits et libertés fondamentaux, Étude annuelle du Conseil d'État*. Paris, 2014.

Rouvroy, Antoinette. « Homo juridicus est-il soluble dans les données? » *Law, Norm and Freedoms in Cyberspace/ Droit, norms et libertés dans le cybermonde: Liber Amicorum Yves Poullet*, 2018, 415-42.

Sagnières, Louis. « La démocratie à l'heure de l'internat : Autonomie politique, vie privée et espace public dans un environnement numérique ». Université de Montréal, 2015.

Schermer, Bart W, Bart Custers, et Simone Van Der Hof. « The crisis of consent: how stronger legal protection may lead to weaker consent in data protection ». *Ethics and Information Technology* 16 (2014). https://doi.org/10.1007/s10676-014-9343-8.

Schoeman, Ferdinand David. *Philosophical Dimensions of Privacy: An Anthology*. *Philosophical Dimensions of Privacy*. Cambridge University Press, 1984.

Schulze, Elizabeth. « Facebook says it got users' permission to share data - users disagree ». *CNBC*, décembre 2018.

Solove, Daniel J. « Privacy: A Concept in Disarray ». In *Understanding Privacy*, 1-11. Harvard University Press, 2008.

Solove, Daniel J. « The Myth of the Privacy Paradox ». *SSRN Electronic Journal* 89, nº 1 (2020): 1-51. https://doi.org/10.2139/ssrn.3536265.

Statistique Canada. « Canadian's assessments of social media in their lives », 2018. https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm.

Swant, Marty. « The 2020 World's Most Valuable Brands ». *Forbes Media*, juillet 2020. https://www.forbes.com/the-worlds-most-valuable-brands/#579b01b4119c.

Thomson Jarvis, Judith. « The Right to Privacy ». *Philosophy & Public Affairs* 4, nº 4 (1975): 295-314.

Toqueville, Alexis de. *De la démocratie en Amérique, II*. Éditions Gallimard, 1961.

ur Rehman, Ikhlaq. « Facebook-Cambridge Analytica data harvesting: What you need to know ». *Library Philosophy and Practice (e-journal)*, 2019.

Véliz, Carissa. « Privacy is Power ». édité par Kindle Edition, 2021.

Véliz, Carissa. « The Internet and Privacy ». *Ethics and the Contemporary World*, 2019.

Warren, Samuel D, et Louis D Brandeis. « The Right to Privacy ». *Harvard Law Review* 4, nº 5 (1890): 193-220.

Warren, Tom. « Amazon explains how Alexa recorded a private conversation and sent it to another user - The Verge ». *The Verge*, mai 2018. https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation.

Législation et jurisprudence

Charte des droits et libertés de la personne, RLRQ c C-12.

Code civil du Québec, RLRQ c CCQ-1991.

Conseil constitutionnel, 12 juin 2018, Décision n° 2018-765 (France) référant au Rapport n°350 (Sénat) de Mme Sophie Joissains, fait au nom de la commission des lois, deposé le 14 mars 2018.

La Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21).

Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, L.Q. 2021, c. 25

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1

Loi sur la laïcité de l'État, RLRQ c L-0.3

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5

Mascouche (Ville) c. Houle, 1999 CanLII 13256 (QC CA).