Penser le droit à la vie privée au regard des droits individuels et collectifs

Projet de recherche financé par le Commissariat à la protection de la vie privée du Canada dans le cadre du Programme des contributions 2021-2022

Rapport de recherche déposé par Jocelyn Maclure, professeur au département de philosophie de l'Université McGill, et Sylvain Auclair, enseignant de philosophie au Cégep de Sainte-Foy et doctorant à la Faculté de philosophie de l'Université Laval

Les personnes suivantes ont contribué à la production de ce rapport :

Samuel Genest, avocat et étudiant à la maîtrise en philosophie à l'Université Laval

Léonard Bédard, étudiant au baccalauréat en philosophie à l'Université Laval

Conclusions du rapport précédent (2020-2021)

Ce présent rapport poursuit les travaux amorcés avec le premier rapport « Droit à la vie privée : analyse conceptuelle et réflexion éthique sur sa source, sa portée et son redéploiement à l'ère des technologies axées sur les données » remis au Commissariat à la protection de la vie privée du Canada dans le cadre du Programme des contributions 2020-2021. La présente section rappelle les principaux éléments mis en lumière dans ce premier rapport.

Les outils d'analyse prédictive sont maintenant utilisés pour inférer des attributs personnels et pour prédire le comportement humain à partir de vastes quantités de données issues de sources variées, notamment des données produites en continu sur Internet. Plusieurs recherches démontrent en effet que ces outils peuvent servir à inférer des renseignements considérés privés et sensibles à partir de données qui sont anodines lorsque prises isolément, mais qui, par regroupement avec d'autres données, révèlent les opinions politiques, les croyances religieuses, l'orientation sexuelle, le mode de vie, l'état de santé ou les traits de personnalité.

Les atteintes à la vie privée ont été traditionnellement définies en termes d'accès, de partage ou d'utilisation d'un renseignement personnel—donc identificatoire—sans le consentement de la personne concernée. Avec les inférences algorithmiques, les préoccupations pour la vie privée se rapportent plutôt à la manière dont des informations personnelles et sensibles sont *générées* par d'autres personnes ou par des organisations à partir d'informations qui sont anodines lorsque prises séparément.

Les inférences algorithmiques peuvent être employées à des fins relativement banales. Plusieurs auteurs expriment toutefois leurs craintes relativement aux risques de biais, de profilage, de discrimination et de manipulation des opinions ou des comportements qu'engendre cette connaissance émergente et dénoncent le contrôle qui peut être exercé sur la vie des personnes. Récemment, plusieurs chercheurs se sont intéressés à la catégorie de préjudices nommée « *predictive privacy harms* ».

Les cadres actuels de protection de la vie privée sont essentiellement basés sur le paradigme du contrôle individuel. Ils consistent à fournir aux individus des mesures leur permettant de contrôler la collecte, l'utilisation et la communication de leurs renseignements personnels, notamment au moyen du consentement. Or, dans le contexte de l'analyse prédictive et des données massives, il devient de plus en plus difficile, voire même impossible, pour un individu de contrôler efficacement les renseignements personnels le concernant et de se protéger contre les préjudices découlant de l'analyse prédictive.

Face aux défis que présente l'analyse prédictive de données massives, nous avons envisagé dans le rapport précédent la proposition selon laquelle la protection de la vie privée devrait focaliser

davantage sur l'encadrement des utilisations des renseignements inférés au regard de leur impact sur les personnes plutôt que sur l'encadrement des pratiques de collecte des renseignements personnels. Des travaux sur les pratiques inacceptables du traitement des données ont été menés par le Commissariat à la protection de la vie privée du Canada. Dans le document d'orientation de 2018 pour l'application du paragraphe 5 (3) de la LPRPDE, des « fins inacceptables » ou « zones interdites » sont identifiées, c'est-à-dire des utilisations de renseignements personnels qu'une personne raisonnable estimerait inacceptables dans les circonstances. Toutefois, une réflexion sur les finalités interdites dans le contexte des renseignements inférés n'a pas été menée jusqu'à maintenant.

Le rapport qui suit sera l'occasion d'approfondir cette proposition. S'il est question d'encadrer les utilisations des renseignements inférés au regard de leur impact sur les personnes, nous avancerons que les utilisations devraient être limitées en fonction des risques de préjudices (*harms*) qu'elles présentent. Nous réaliserons une analyse critique de la théorie de l'intégrité contextuelle proposée par Helen Nissenbaum et qui semble un cadre théorique prometteur afin d'identifier des utilisations de renseignements inférés qui ne seraient pas acceptables au regard de leurs risques. Au cours de notre analyse, nous formulerons des précisions sur la relation entre le droit à la vie privée et les droits fondamentaux et sur la dimension collective de la protection de la vie privée.

Présentation de la théorie de l'intégrité contextuelle de Nissembaum

Théorie de l'intégrité contextuelle et définition du droit à la vie privée

Ce sont les enjeux de vie privée découlant de l'utilisation de données disponibles dans la sphère publique qui ont motivé la philosophe et professeure en sciences de l'information à Cornell Tech, Helen Nissenbaum, à élaborer sa théorie de l' « intégrité contextuelle ». Dans son article de 1998 « Protecting Privacy in an Information Age : The Problem of Privacy in Public », Nissenbaum fait remarquer que les théories philosophiques et juridiques de la vie privée se sont attardées aux informations personnelles, intimes et sensibles, en partant du principe que les cadres de protection de la vie privée ne s'appliquent pas aux renseignements provenant de la sphère publique. Or, soutient Nissenbaum, « information and communications technology, by facilitating surveillance, by vastly enhancing the collection, storage, and analysis of information, by enabling profiling, data mining and aggregation, has significantly altered the meaning of public information » (Nissenbaum 1998, p. 559). Les données publiées sur Internet ou les données rendues disponibles dans des banques publiques peuvent soulever des enjeux de vie privée. C'est pourquoi, explique-t-elle, « a satisfactory legal and philosophical understanding of a right to privacy, capable of protecting the important values at stake in protecting privacy, must incorporate, in addition to traditional aspects of privacy, a degree of protection for privacy in public ». C'est principalement pour répondre à ce besoin que Nissenbaum a élaboré sa théorie de

l'intégrité contextuelle. Le livre *Privacy in Context: Technology, Policy, and the Integrity of Social Life* publié en 2010 développe des idées que Nissenbaum avait déjà exposées dans des articles.

> Motivating this book is the challenge of socio-technical systems and practices that have radically altered the flow of information and thereby affected institutions, power structures, relationships, and more. Conceptions that have served adequately until now are, in my view, unable to adapt to the new landscape […] I am not as concerned with capturing the full meaning of privacy but with precisely and systematically characterizing the nature of these radical alterations. Most importantly, I am interested in addressing the question of when and why some of these alterations provoke legitimate anxiety, protest and resistance. In applying contextual integrity to this question, I call on it to serve as a decision heuristic, a framework for determining, detecting, or recognizing when a violation has occurred (p. 148).

Nissenbaum annonce que sa préoccupation première, avec sa théorie, n'est pas de cerner la nature du droit à la vie privée. Elle laisse de côté les préoccupations plus abstraites au sujet de la définition de la vie privée afin de s'intéresser plutôt aux problèmes de vie privée soulevés par les nouvelles technologies. Bien que Nissenbaum propose une certaine compréhension du droit à la vie privée, sa théorie de l'intégrité contextuelle doit être avant tout comprise comme un cadre théorique ou un outil servant à identifier les atteintes possibles au droit à la vie privée, en vue de permettre la mise en place de protections légales adéquates.

Dans son article publié en 2021 « What is Privacy ? That's the Wrong Question », Woodrow Hartzog explique que la théorie de Nissenbaum s'inscrit dans la lignée de l'approche centrée sur les problèmes défendue par le professeur de droit Daniel Solove. Alors que les travaux des théoriciens du 20e siècle ont principalement porté sur la formulation d'une définition du droit à la vie privée, des penseurs, dont Solove, ont récemment adopté une approche plus pratique centrée sur les problèmes de vie privée. « In an ongoing series of articles and books starting in 2001, Solove worked to reshape the entire narrative around privacy by suggesting that we stop obsessing over what privacy is and start asking what privacy is for » (Hartzog, 2021, p. 1679). Afin de mieux comprendre la perspective centrée sur les problèmes adoptée par Nissenbaum, nous passerons en revue les principales idées avancées par Solove pour défendre cette perspective. Nous examinerons aussi la thèse réductionniste défendue par la philosophe Judith Thomson et les critiques de cette thèse.

Une approche centrée sur les problèmes de vie privée

Dans son livre publié en 2008 *Understanding Privacy*, Solove explique en ces mots ce qu'il nomme l'approche « traditionnelle » du droit à la vie privée :

> The majority of theorists conceptualize privacy by defining it *per genus et differentiam*. In other words, theorists look for a common set of necessary and sufficient elements

> that single out privacy as unique from other conceptions. Although the terminologies theorists employ differ, most theorists strive to locate the 'essence' of privacy–the core common denominator that makes things private. The traditional method endeavors to conceptualize privacy by constructing a category that is separate from other conceptual categories (such as autonomy and freedom) and that has fixed, clear boundaries so we can know when things fall within or outside the category (p. 14).

Passant en revue les principales définitions avancées par les théoriciens, Solove explique que ces définitions sont insatisfaisantes, étant trop étroites ou trop larges.

> Any attempt to locate a common denominator for all the manifold things that fall under the rubric of 'privacy' faces an onerous choice. A common denominator broad enough to encompass nearly everything involving privacy risks being overinclusive or too vague. A narrower common denominator risks being too restrictive (p. 37).

Solove n'est pas le seul à insister sur les difficultés de cerner la définition du droit à la vie privée. Judith DeCew (1997), par exemple, affirme que « it is not possible to give a unique, unitary definition of privacy that covers all the diverse privacy interests […] privacy is a broad and multifaceted notion that is best understood in terms of a 'cluster concept' ». Robert C. Post (2001), pour sa part, « has argued that it is extremely difficult, if not impossible, to succeed in this endeavor of defining the right to privacy's essence ». Constatant que « perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is », Judith J. Thomson a fourni la critique la plus radicale à l'égard des tentatives de définir le droit à la vie privée. Défendant une thèse réductionniste, Thomson affirme que les violations habituellement associées au droit à la vie privée peuvent être tout aussi bien expliquées en termes de violations d'autres droits. Puisque le droit à la vie privée peut être expliqué par d'autres droits, il devient inutile de faire appel à celui-ci, voire d'en faire la simple mention en vue d'en dénoncer la violation ou d'en justifier la protection. Attardons-nous un instant à la thèse réductionniste défendue par Thomson et aux critiques qui ont été formulées à l'égard de sa thèse.

Dans son article « The Right to Privacy » publié en 1975, Thomson écrit que :

> […] nobody seems to have any very clear idea what the right to privacy is. We are confronted with a cluster of rights-a cluster with disputed boundaries-such that most people think that to violate at least any of the rights in the core of the cluster is to violate the right to privacy; but what have they in common other than their being rights such that to violate them is to violate the right to privacy […]
>
> That we feel the need to find something in common to all of the rights in the cluster and, moreover, feel we haven't yet got it in the very fact that they are all in the cluster, is a

> consequence of our feeling that one cannot explain our having any of the rights in the cluster in the words: "Because we have a right to privacy."
>
> But then if, as I take it, every right in the right to privacy cluster is also in some other right cluster, there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster and no need to settle disputes about its boundaries. 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. Indeed, the wrongness of every violation of the right to privacy can be explained without ever once mentioning it.

Thomson présente une série de situations qui sont intuitivement reconnues comme des atteintes au droit à la vie privée et soutient que ces atteintes sont avant tout des atteintes à d'autres droits, en particulier le droit de propriété et les droits sur la personne (*right over the person*). Elle donne l'exemple d'une personne qui ne souhaite pas rendre publique une image pornographique qu'elle détient. La personne, explique Thomson, possède le droit exclusif de l'observer, de la cacher, d'en disposer, etc. L'aspect propre de la « possession » permet à Thomson de reconnaître tout un ensemble de droits dérivés de celle-ci. Nous pourrions être tentés de parler ici d'une « intimité » désirée par l'individu en question. Or, cette intimité – et éventuellement le droit à la vie privée qui lui est associé – provient plutôt selon Thomson du droit à la propriété qui permet de se réclamer de ladite intimité. C'est précisément parce que l'individu possède l'image qu'il peut en faire ce que bon lui semble et qu'il peut se réclamer d'une violation de son « intimité » si une tierce partie l'observe à son tour. En ce sens, Thomson considère que l'on peut dériver le droit à la vie privée du droit à la propriété. Cette disposition à considérer la vie privée relativement à la propriété possède néanmoins ses limites ayant trait à la *personne*. Elle mettra de l'avant ce qu'elle appelle des « droits sur la personne » (*rights over the person*). Ces droits impliquent, par exemple, le droit de ne pas être vu, ou ne pas être entendu sans son consentement préalable. Ce sont ces droits qui sont en jeu lorsqu'une personne est par exemple espionnée dans sa cuisine le soir. Thomson précise que « these rights – the right to not be looked at and the right to not be listened to – are analogous to rights we have over property ». Ces deux types de droits s'exercent de différentes manières, mais participent tous deux à dériver un « droit à la vie privée » en ceci que c'est parce que nous nous possédons « corporellement », ou que nous possédons un objet et que nous choisissons d'en faire usage, que nous établissons la dimension « privée » à notre vie et que nous dérivons un droit en conséquence. Comprendre ces droits permet à Thomson de traiter de ce que nous pourrions rattacher à une vie privée informationnelle. Ainsi qu'elle l'indique :

> A great many cases turn up in connection with information. […] You may violate a man's right to privacy by looking at him or listening to him; there is no such thing as violating a man's right to privacy by simply knowing something about him. […] We have a right that certain steps shall be taken to find our facts, and we have a right that certain uses shall not be made of facts (p. 5).

Le fait qu'une entité – individu ou entreprise – connaisse un ensemble de faits sur un individu sans que celui-ci n'y ait consenti relève ainsi d'une atteinte à son droit à la vie privée par son « droit de ne pas être regardé ». Cette atteinte renvoie aux « droits sur la personne » et, par extension, au droit à la vie privée.

Notons au passage que la philosophe américaine Amy Peikoff offre une défense contemporaine du réductionnisme de Thomson, notamment au sein de son article « Beyond Reductionism : Reconsidering the Right Privacy » publié en 2008. Selon Peikoff, le principe d'échanges mutuels en cours dans nos sociétés permet de conclure que : « property rights are more fundamental that the right to privacy because people are inclined to explain the wrongness of invasions of privacy in terms of property rights » (p. 17). Peikoff va même jusqu'à évacuer les droits sur la personne mentionnés par Thomson, en rapportant ceux-ci à la propriété corporelle : c'est parce que « je possède mon corps » que je peux décider qui entend mes paroles. Concevoir la vie privée autrement que par dérivation du droit à la propriété représenterait selon elle un risque de dérive, car il s'agirait d'une protection d'une forme négative du droit à l'action par la restriction d'une action. Selon Peikoff, cela serait contradictoire avec la visée objectiviste du droit qu'elle propose et qui doit reposer sur des évènements perceptibles.

La thèse réductionniste a été l'objet de critiques. Dans son article « Why Privacy Is Important? » de 1975, James Rachels soutient qu'il y a des liens étroits entre notre habileté à contrôler l'information à notre propos et notre habileté à contrôler nos relations sociales. Ce qui relève de la vie privée, et plus foncièrement, du droit à la vie privée réside dans notre capacité à contrôler le type de relations sociales que l'on désire avec les personnes que l'on souhaite. Or, en dérivant le droit à la vie privée du droit à la propriété – et des droits à travers la personne –, Thomson protège la corporalité (et sa possession), précisément puisqu'elle est nôtre, au même titre que toutes autres formes de propriétés. Elle ira jusqu'à justifier un « droit de ne pas être regardé » à l'aide de cette conception dérivative du droit à la vie privée. Cela dit, tel qu'elle est vécue au quotidien, l'intimité physique est, aux dires de Rachels, partie prenante d'une relation beaucoup plus profonde avec notre propre corporalité que sa simple possession.

Ce caractère « unique » à l'intimité que tendrait à protéger la vie privée fait également l'objet de la critique qu'offre Jeffrey Reiman à l'égard de Thomson au sein de « Privacy, Intimacy, and Personhood » (1976). La force de ces critiques réside probablement dans leur capacité à identifier le caractère intime propre à la vie privée, ce que Thomson n'arrive pas à faire. Certains penseurs, dont William A. Parent (1983), reprochent à Thomson le fait qu'elle fournisse un ensemble d'exemples de violation de la vie privée qui suppose une certaine conception sans jamais fournir une définition de ce droit :

> The basic failing of Thomson's essay is that she makes no attempt to define privacy. We have good reasons to ask how she hopes to convince

> anyone that the right to privacy is derivative and quite dispensable without first telling us what the right means (p. 280).

Julie Inness (1996) démontre que, s'il est indéniable qu'accéder à la possession d'autrui sans son consentement constitue une atteinte à sa vie privée, cela n'est pas nécessairement une atteinte au droit à la propriété. Pour cette philosophe du droit, les droits à travers la personne et le droit de propriété ne sont pas une condition suffisante en vue d'en dériver un « droit à la vie privée ». Tel qu'elle l'indique :

> We commonly think of property rights as the right to sell possessions and the right that others do not sell those possessions without permission. On the surface, property rights do not include such privacy rights as the right not to have a pornographic picture examined. More generally, it is not immediately obvious that ownership rights entail any privacy claims, claims involving restricting another's ''sensing'' of possessions. Thomson views this intuitive separation between property and privacy claims as product to carelessness or conceptual confusion. According to her, privacy claims to restrict access to something in the external world amount to nothing more than property rights (p. 5).

En reprenant l'exemple de « l'image pornographique » de Thomson, Inness démontre que, par son caractère dérivatif propre à la thèse réductionniste, le droit à la vie privée devient vulnérable à une simplification normative menant à l'abandon complet de toute discussion relative à ce droit. Néanmoins, il demeure possible pour Inness d'explorer les revendications propres à « la vie privée ». Prétendre le contraire, tel que le fait Thomson, cherche à nier des intuitions communes fortes. Même s'il est indéniable qu'accéder à une possession d'autrui sans son consentement peut constituer une atteinte à sa vie privée, il faut faire attention, nous dit Inness, à se questionner si cette atteinte constitue une violation directe d'un *droit à la propriété*, et plus largement, d'un *droit à l'égard de la personne*. Question de mieux illustrer le tout, prenons la situation de Mathilda et Félix, tous deux camarades de classe. Un beau matin, Félix rédige en classe une lettre d'amour destinée à Mathilda. Or, une fois que celui-ci le lui a donné, elle ne peut s'empêcher de la recopier et de la montrer à ses amies. Félix dit à Mathilda qu'elle porte atteinte à sa vie privée. A-t-il raison d'affirmer une telle chose? Pour Inness, il serait tout à fait justifié d'affirmer la violation de ce droit, considérant que le droit à la vie privée peut être détaché de la possession en tant que telle. Cela semble d'ailleurs faire appel à nos intuitions communes en la matière. En reprenant l'exemple des deux élèves, la situation serait totalement différente si, plutôt que de lui donner une lettre d'amour, Félix était voisin de bureau de Mathilda, et mettait un stylo au coin de son bureau. Tandis que Félix a le dos tourné, Mathilda regarde discrètement le stylo de Félix avant que celui-ci ne fasse volte-face et lui ordonne d'arrêter de regarder son stylo, pour cause d'une violation de sa vie privée. Une telle justification nous semble toutefois absurde, et ce, malgré que le stylo est sa propriété, *a contrario* de la lettre recopiée préalablement. C'est ce qui fait dire à Inness que la vie privée n'est pas directement et seulement

rattachée au simple fait de la possession. Un problème similaire advient lorsque l'on considère le « droit de la personne » décrit par Thomson qui semble se traduire par un « droit à la possession corporelle », même si cette dernière ne fait pas de précision en ce sens. Imaginons un individu assis dans un compartiment fermé de train. Remarquant un autre individu louche qui tente de l'observer à travers la fenêtre du compartiment, le détenteur de la cabine se cache sous son banc, échappant ainsi au regard de l'étranger qui ne parvient finalement pas à détecter sa présence. Dans ce cas bien précis que nous avons adapté de l'exemple fournit par Inness elle-même, il semble que la vie privée du propriétaire du compartiment ait été bafouée, sans qu'il n'ait souffert d'une quelconque « appropriation de son corps », au même titre que s'il avait été écouté par l'espion sourd de Thomson. La raison est simple : il n'a été ni entendu ni vu. Son corps ne s'est donc pas fait « approprier ».

Thomson prétend que le droit de propriété et les droits sur la personne sont plus fondamentaux et servent d'assise au droit à la vie privée. Pour Inness, il n'y a aucune raison de voir en ces deux droits une « primauté » antérieure à la vie privée. Tel qu'Inness le précise :

> This claim that derivative status of privacy is sufficient grounds to abandon discussion of privacy is fundamentally flawed […] we neglect that the fact that a cluster of derived claims can have a conceptual and normative significance irreducible to the meaning and value of the source from which it was derived.

Plusieurs auteurs ont soutenu que les enjeux de la vie privée informationnelle sont multiples et ne peuvent pas être réduits au droit à la propriété ou aux droits sur la personne ainsi que le pense Thomson. C'est notamment le cas de Thomas Scanlon (1975) qui argumente que :

> not much insights into the problems raised by electronic surveillance or by conflicts between considerations of privacy and the requirements of a free press is to be gained by consulting rights of ownership or even rights of the person in the form in which Thomson presents them (p. 332).

Solove souligne les difficultés à étendre le concept de « propriété » à une information personnelle. Au contraire d'un objet, une information peut être possédée par des millions d'individus de manière simultanée. D'ailleurs, précise-t-il, les lois propres à la propriété intellectuelle encadrent l'expression des idées comme telles plutôt que les idées sous-jacentes elles-mêmes. Il est à noter que plusieurs auteurs ont critiqué la conception de la protection des données qui renvoie à la notion de « données » comme un « avoir » dont le « propriétaire » pourrait négocier l'accès ou non en valeur de sa valeur marchande. Voir notamment le livre *La vie privée à l'heure de la société du numérique* (2019) d'Yves Poullet. Pour Solove, reconnaître une « propriété » à l'information personnelle traduit des difficultés importantes lorsqu'on considère que l'information personnelle émerge en vertu d'une relation avec autrui, ce qui implique de potentielles revendications partagées vis-à-vis la propriété de cette même information. Cet *autrui*

peut être une relation personnelle avec un proche, aussi bien qu'une relation virtuelle avec une entreprise de marketing qui collecte des données. En ce sens, la « valeur marchande » de l'information personnelle ne devient pas uniquement l'objet de son détenteur, mais bien de la création de celle-ci qui peut être multifactorielle. Un exemple récurrent au sein de la littérature est celui de l'algorithme de prédiction de grossesse développé par la compagnie *Target*, tel que rapporté par le journaliste Charles Duhigg en 2012. L'information sur la grossesse de la jeune fille n'a pas été *recueillie*, mais bien *inférée* ou *prédite* ou inférée au moyen d'outils d'analyse sophistiqués et sur la base de corrélations significatives dans une vase quantité de données. Dans ce cas précis impliquant l'utilisation de l'analyse prédictive et de données massives, il serait ainsi difficile pour les individus des échantillonnages de données de se réclamer de la « possession » de leurs portraits constitués à partir de leurs données disséminées.

Dans les exemples présentés par Thomson, les atteintes au droit à la vie privée renvoient à des atteintes déjà couvertes par un autre droit. Toutefois, comme nous l'avons déjà souligné, l'analyse prédictive permet l'inférence de renseignements jugés privés et sensibles (par exemple le fait d'être enceinte, l'état de santé et les opinions religieuses ou politiques) à partir de données rendues publiques et qui sont insignifiantes lorsque prises séparément. S'il on reconnaît qu'il y a atteinte à la vie privée du fait d'inférer des informations reconnues personnelles et sensibles, il n'est pourtant pas clair qu'il existe un droit sur les données publiées et sur leur utilisation. Rappelons que ce sont les enjeux de vie privée découlant de l'utilisation de données disponibles dans la sphère publique qui ont motivé Nissenbaum à élaborer sa théorie de l'intégrité contextuelle.

Pour échapper aux difficultés inhérentes à la recherche d'un dénominateur commun unique de la vie privée que Thomson dénonce, Solove propose de conceptualiser le droit à la vie privée d'une manière différente et en s'inspirant des travaux du philosophe Wittgenstein :

> There is a way out of this dilemma: We can conceptualize privacy in a different way. The philosopher Ludwig Wittgenstein argued that some concepts are best understood as family resemblances – they include things that "are *related* to one another in many different ways" (Wittgenstein 1958: § 65, original emphasis). Some things share a network of similarities without one particular thing in common. They are related in the way family members are related. You might have your mother's eyes, your brother's hair, your sister's nose – but you all might not have one common feature. There is no common denominator. Nevertheless, you bear a resemblance to each other (Solove, 2015, p. 74).

Par exemple, suivant les idées de Wittgenstein, il y a des ressemblances ou des propriétés communes entre le tennis et le badminton qui font en sorte que ces deux jeux font partie de la catégorie « sports de raquette ». Il y a aussi des ressemblances entre les sports de raquette et les jeux de table qui font en sorte qu'ils font partie de la classe « jeux ». Cette approche de Wittgenstein permet de reconnaître les similarités et différences des exemples d'un concept.

Solove soutient qu'une reconstruction de la compréhension même de la vie privée doit être entreprise à partir d'une perspective ascendante, « from the bottom up rather than the top down ». En cela, il dit s'inspirer de l'approche pragmatique du philosophe américain John Dewey selon qui la réflexion philosophique doit partir des problèmes issus de l'expérience plutôt que des principes abstraits. Selon Solove, il est nécessaire de partir des problèmes de vie privée afin de pouvoir penser adéquatement les mesures de protection:

> I argue that the focal point should be on privacy *problems*. When we protect privacy, we protect against disruptions to certain activities. A privacy invasion interferes with the integrity of certain activities and even destroys or inhibits some activities. Instead of attempting to locate the common denominator of these activities, we should conceptualize privacy by focusing on the specific types of disruption (Solove, 2008, p. 9)

Solove propose une taxonomie de seize activités susceptibles de créer des problèmes de vie privée et qui sont regroupées sous les quatre catégories suivantes : collecte de l'information, traitement de l'information, diffusion de l'information et invasion. La valeur de la vie privée dépend de l'importance de ces activités pour l'individu et la société. Dans son livre, Solove explique en quoi chacun des problèmes est distinct des autres problèmes et en quoi les problèmes sont reliés ensemble, dans la perspective des ressemblances de famille de Wittgenstein. Toutefois, force est de reconnaître que le lien de ressemblance n'est pas toujours évident entre les problèmes présentés.

Les préjudices (*harms*) occupent une place importante dans la taxonomie de Solove. Un problème, précise Solove, est « a situation that creates harms to individual and society » (p. 174). Un problème de vie privée peut engendrer plusieurs préjudices. Solove affirme que « the theory of privacy I have developed aims to improve our ability to recognize and comprehend the harms created by privacy problems » (p. 174). Dans une version préliminaire (2021) d'un article à paraître en 2022, Solove présente avec Daniel Keats Citron une liste révisée des préjudices à la vie privée (*privacy harms*). Nous reviendrons plus loin dans ce rapport sur la liste des préjudices de Solove et de Citron.

Suivant l'approche pragmatique, l'analyse du contexte importe. « In any given case, we need to resolve privacy issues by looking to the specific context » (Solove 2008, p. 48). Le contexte est un aspect essentiel de la conceptualisation de la vie privée. Toutefois, il n'est pas clair ce que Solove signifie par « looking to the specific context ».

La théorie de Nissenbaum partage avec Solove une préoccupation pour les problèmes liés au droit à la vie privée. Tout comme pour Solove, le point de vue est pratique : il importe d'ajuster la protection de la vie privée en réponse à ces problèmes. La recherche d'une définition de la vie privée est secondaire. La contribution de la théorie de l'intégrité contextuelle se situe sur le plan de la compréhension du contexte et du cadre d'analyse qu'elle propose afin de penser les problèmes de vie privée.

La théorie de l'intégrité contextuelle et les théories du contrôle et de l'accès

Nissenbaum a développé un cadre théorique permettant de déterminer quand une nouvelle technologie porte atteinte à la vie privée et d'identifier les attentes des personnes au regard de leur vie privée. Elle précise d'ailleurs que la doctrine de l'attente raisonnable en matière de vie privée est étroitement liée, sur le plan conceptuel, à la théorie de l'intégrité contextuelle.

Nissenbaum observe que nous sommes entourés d'une quantité importante de flux d'informations qui, d'une part, peuvent menacer notre vie privée, mais, d'autre part, sont également nécessaires pour de nombreux services essentiels ou utiles. Elle propose une façon de théoriser la fonction et la valeur de la vie privée à une époque où les données sont générées, diffusées et analysées à un rythme si rapide que le contrôle individuel sur les données semble ne pas toujours être possible. Au-delà du fait qu'il y a ou non flux de renseignements personnels, ce qui importe pour la protection de la vie privée, explique Nissenbaum, c'est que le flux soit approprié.

> Many argue that that protecting privacy means strictly limiting access to personal information or assuring people's right to control information about themselves. I disagree. What people care most about is not simply restricting the flow of information but ensuring that it flows appropriately, and an account of appropriate flow is given here through the framework of contextual integrity (Nissenbaum, 2010, p.…).
>
> We have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met (Nissenbaum, 2010, p. 231).

Ainsi, dès le début de son livre, Nissenbaum tient à distinguer sa théorie sur la vie privée de deux théories qui ont exercé une influence importante, soit la théorie du contrôle et la théorie de l'accès. La théorie du contrôle se concentre sur la capacité de l'individu à exercer un contrôle sur ses informations personnelles, de choisir ce qu'il partage comme informations. La théorie de l'accès affirme que « la vie privée ne relève pas exclusivement d'un contrôle de la personne sur ses renseignements personnels, mais de la capacité à cette personne à limiter l'accès que les autres ont à certaines dimensions de sa vie » (Benyekhlef et Déziel 2018, p. 26 et 29).

Chacune de ces théories sur la vie privée propose une conception différente de la protection de la vie privée en matière de renseignements personnels, ainsi que l'explique Mark Burdon dans son livre *Digital Data Collection and Information Privacy Law* (2020) :

> […] different concepts of information privacy provide different emphases about what information privacy law should protect. **Control concepts** emphasise the requirement

> for individually oriented mechanisms, processes and rights. **Informational access considerations** promote private zones that allow the flourishing of autonomous individuals as a founding precept of liberal society. Control and access therefore represent the initial root structure of information privacy's conceptual entanglement with broader privacy concepts. However, even while these roots begin to take substantial hold, a new conceptual root system starts to develop that critiques both the individualised aspects of control and the liberal perfumery of the autonomy justifications of information privacy. This contemporary root system gathers from different directions but formulates broadly around a key idea – namely, that the practices of privacy and information privacy are situated in social and political contexts. Contemporary concepts thus highlight the **social and relational context of information privacy**, which leads to the construction of new forms of critique, including critical appraisal of the very process of conceptualisation of information privacy (p. 121).

Nous déjà souligné les limites de la théorie du contrôle dans le contexte de l'analyse prédictive. Nissenbaum n'est pas en accord avec l'idée mise de l'avant dans la théorie de l'accès, à savoir que protéger la vie privée consiste essentiellement à limiter l'accès aux renseignements personnels. Ce qui compte, plutôt, c'est que le flux de renseignements personnels soit « approprié ». Sa position dépend ainsi lourdement de ce qui est entendu par « flux de renseignements » et des critères permettant son évaluation normative, c'est-à-dire des critères nous permettant d'évaluer si un flux particulier est « approprié ».

Selon Nissenbaum, les théories du contrôle et de l'accès offrent des points de vue limités pour la protection de la vie privée. Nous constaterons plus loin qu'ils réfèrent à deux des possibles *principes de transmission* de la théorie de Nissenbaum.

Concepts de la théorie de l'intégrité contextuelle de Nissenbaum

Nissenbaum formule ainsi le but de sa théorie :

> The framework of contextual integrity provides a rigorous, substantive account of factors determining when people will perceive new information technologies and systems as threats to privacy; it not only predicts how people will react to such systems but also formulates an approach to evaluating these systems and prescribing legitimate responses to them (Nissenbaum 2010, p. 2).

> we take privacy to be the requirement that information about people ('personal information') flows appropriately, where appropriateness means in accordance with informational norms. Barocas et Nissenbaum 2014, p. 47)

Les atteintes à la vie privée ne se produisent pas exclusivement lorsque les gens n'ont pas le contrôle des données ou encore lorsque trop de données circulent. Plus généralement, les gens

perçoivent qu'il y a une atteinte à la vie privée lorsque le flux d'informations personnelles est *inapproprié*, c'est-à-dire lorsque la circulation des informations personnelles contrevient aux « normes contextuelles d'information ». La théorie de l'intégrité contextuelle insiste sur l'importance du contexte. À cet égard, Nissenbaum n'est pas la première. Plusieurs penseurs avant Nissenbaum ont insisté sur la nécessité de contextualiser la vie privée afin de l'évaluer. Elle le reconnaît elle-même : « I am not inventing the idea of social context. Instead, I rely on a robust intuition rigorously developed in social theory and philosophy that people engage with one another not simply as human to human but in capacities structured by social spheres » (p. 130). Du point de vue juridique, l'arrêt *R. c. Edwards*, [1996] 1. R.C.S. 128 de la Cour suprême du Canada précise que la détermination d'une attente raisonnable en matière de vie privée requiert une approche contextualisée, comme c'est généralement le cas lorsqu'il s'agit d'évaluer les atteintes aux droits protégés par la Charte canadienne des droits et libertés. La théorie de l'intégrité contextuelle de Nissenbaum est toutefois reconnue comme étant « l'énoncé conceptuel le plus clair de l'importance du contexte social dans l'application de la loi sur la protection des renseignements personnels » (Burdon, p. 122). L'apport de Nissenbaum se trouve dans l'analyse qu'elle propose du contexte et en particulier du côté de son concept central : les « normes contextuelles d'information ». « The heart of the framework of contextual integrity is an elaboration of its key construct: context-relative informational norms » (Nissenbaum 2010, p. 129).

La société, fait remarquer Nissenbaum, est composée de divers contextes, c'est-à-dire de différentes situations sociales, par exemple, l'éducation, les soins de santé, l'amitié et les échanges commerciaux. Chaque contexte est structuré autour d'un ensemble de normes, c'est-à-dire de règles qui guident la vie sociale au sein de ces contextes et qui déterminent les attentes des gens. Ces normes sont en jeu lorsque les gens consultent un médecin, suivent un cours à l'école ou discutent avec un ami. L'intégrité contextuelle est fondée sur le contexte social et trouve son expression dans son concept, soit les « normes contextuelles d'information ». Ces normes régissent les flux de renseignements personnels dans la vie quotidienne et orientent les attentes des gens au regard de la vie privée. Par exemple, bien qu'il puisse être approprié de divulguer des détails de sa vie sexuelle à un médecin lorsqu'on le consulte à ce sujet, il ne serait pas approprié d'avoir à divulguer ces mêmes informations à un employeur dans le cadre d'un processus d'embauche. Selon la théorie de l'intégrité contextuelle, la vie privée est respectée lorsque les renseignements personnels circulent sans enfreindre les normes contextuelles d'information.

Ces normes, explique Nissenbaum, sont définies par les paramètres clés suivants :

- les **acteurs impliqués**, catégorie qui renvoie au **sujet**, à l'**expéditeur** et le **destinataire** dont les rôles varient selon le contexte

- le **type d'information en question** (par exemple : le diagnostic médical, l'opinion politique, les résultats d'apprentissage)

- le **principe de transmission en jeu** qui énonce la condition appliquée au flux d'information. Par exemple, le contrôle sur ses informations, la confidentialité, le consentement ou la réciprocité.

Afin d'évaluer si une pratique donnée respecte ou viole la vie privée, les flux d'informations associés à cette pratique sont décrits en attribuant des valeurs à chacun de ces cinq paramètres. Par exemple, dans le contexte des soins de santé, il est communément admis que les patients (expéditeur et sujet) fournissent à leur médecin (destinataire) des informations de santé (attribut) en toute confiance et confidentialité (principe de transmission). Une pratique qui génère des flux de données conformes ne pose pas de problème. En revanche, si une pratique détourne des informations médicales vers un autre destinataire, par exemple l'employeur du patient, un signal d'alarme est émis, même si tous les autres facteurs restent inchangés. Aussi, si l'un des paramètres n'est pas spécifié, la description est ambiguë.

Pour prendre un autre exemple, imaginons que vous demandez un prêt bancaire pour une nouvelle maison et que vous avez signé une renonciation autorisant la banque à obtenir une copie de votre dossier de crédit auprès d'une société (par exemple, Equifax). Vous êtes le sujet, la banque est le destinataire des données alors que le bureau de crédit est l'expéditeur. Le type d'information comprend les différents champs d'information qui sont fournis dans le rapport de crédit. Le principe de transmission est « avec le consentement signé par la personne concernée ».

Notons que les cinq paramètres clés sont indépendants. Aucun d'entre eux ne peut être réduit aux deux autres et aucun d'entre eux ne suffit pour déterminer les attentes en matière de protection de la vie privée.

Le paramètre « principe de transmission » désigne les conditions ou les contraintes suivant lesquelles l'information circule. Nissenbaum explique que le principe de transmission n'a pas été reconnu explicitement dans les réflexions universitaires sur la vie privée même si, dans la pratique, son rôle est implicite dans les conventions sociales, les règlements et les lois. Selon Nissenbaum, isoler le principe de transmission en tant que variable indépendante permet également de rendre compte de manière plus générale de la vision dominante du droit à la vie privée comme un droit de contrôler les informations nous concernant. Nissenbaum fait remarquer que définir la vie privée en tant que *contrôle de l'individu sur ses renseignements personnels* est une vision réductrice dans la mesure où le contrôle n'est qu'un des principes de transmission possibles et que sa pertinence doit être évaluée selon le contexte et les autres paramètres impliqués.

La théorie de l'intégrité contextuelle comporte un premier niveau descriptif. Il s'agit, pour chacune des situations examinées, de décrire les paramètres clés qui caractérisent les normes contextuelles d'information et constater si la nouvelle technologie dont il est question modifie l'un des paramètres clés actuellement en vigueur.

> According to the theory of contextual integrity, the appropriateness of a particular information flow depends not only on the type of information in question (the attribute) but also on the actors involved (senders, subjects and recipients of an information type) and the transmission principles (constraints on flow). If a practice generates changes in any of these three parameters, a prima facie case exists for claiming that contextual integrity, and hence privacy, has been violated (Nissenbaum et Kift 2017).

Le flux d'informations conforme aux normes contextuelles d'information est présumé approprié. Le flux qui n'est pas conforme à ces normes est présumé inapproprié. Cependant, la description n'est que le premier niveau et ne peut pas être la fin de l'analyse. Les normes changent en réponse à l'évolution des conditions sociales et des technologies. D'ailleurs, en leur temps, les juristes Warren et Brandeis étaient scandalisés par l'émergence de l'appareil photo qui pouvait prendre des photographies en un instant. Aujourd'hui, nous acceptons ces appareils sans arrière-pensée. Une théorie de la vie privée qui proscrirait toutes les pratiques de données incompatibles avec les normes informationnelles existantes serait inutilement conservatrice et empêcherait l'introduction de nouvelles technologies qui sont hautement bénéfiques à l'humanité. À ce premier niveau descriptif, Nissenbaum ajoute un deuxième niveau normatif afin de tracer la ligne entre, d'une part, les pratiques de données transgressant les normes qui sont légitimes et, d'autre part, les pratiques de données transgressant les normes qui ne le sont pas.

> This prima facie assessment does not necessarily mean, however, that the new practice needs to be abandoned. Indeed, if the new practice better promotes the values, goals and ends of a given context, then contextual integrity allows for and even encourages alterations in information flows (Nissenbaum et Kift 2017).

À ce deuxième niveau qui est normatif, il faut se demander si la pratique qui transgresse les normes contextuelles d'information promeut des valeurs morales, politiques et spécifiques au contexte (par exemple, l'équité, la justice, la liberté, l'autonomie) mieux que les pratiques existantes et conformes à ces normes. Si c'est le cas, cela peut rendre le nouvel usage de données légitime et approprié malgré le fait qu'il enfreigne les normes contextuelles d'information existantes.

> A fundamental insight of contextual integrity is that because information flows may systematically affect interests and realization of societal values, these can be used as touchstones for normative evaluation. Where novel flows challenge entrenched informational norms, the model calls for a comparative assessment of entrenched flows against novel ones. An assessment in terms of interests and values involves three layers. In the first, it requires a study of how novel flows affect the interests of key affected parties: the benefits they enjoy, the costs and risks they suffer […] Beyond this largely economic analysis, frequently followed in policy circles, the normative analysis directs us to consider general moral, social, and political values […] Core ethical and societal

> values have been identified in a deep and extensive privacy literature […] The third layer introduces a further set of considerations, namely, context-specific values, ends, and purposes […] This layer insists that privacy, as appropriate information flows, serves not merely the interests of individual information subjects, but also context, social ends, and values (Nissenbaum, 2010, p. 289-290).

Nissenbaum présente une heuristique décisionnelle (*decision heuristic*) prête à être appliquée afin d'évaluer des nouvelles technologies au regard du caractère approprié du flux d'informations personnelles (heuristique tirée de Nissenbaum, 2010, p. 182).

1. Identifier la nouvelle pratique en termes de flux d'informations. Le type d'information en question doit être identifié. Par exemple, dans le domaine de la santé, il peut s'agir de diagnostics médicaux ou de maladies. Dans le domaine de l'éducation, il peut s'agir de mesures de performance ou de résultats d'apprentissage.

2. Identifier le contexte dominant. Établir le contexte à un niveau de généralité familier (par exemple, "soins de santé") et identifier les impacts potentiels des contextes qui lui sont imbriqués, comme "hôpital universitaire".

3. Identifier le sujet de l'information, les expéditeurs et les destinataires.

4. Identifier les principes de transmission.

5. Repérer les normes informationnelles enracinées applicables et identifier les points de départ importants.

6. Jugement *prima facie* : Il peut y avoir plusieurs façons pour un système ou une pratique de défier les normes établies, en particulier un ou plusieurs des paramètres clés [...] Une violation des normes informationnelles donne lieu à un jugement *prima facie* que l'intégrité contextuelle a été violée parce que la présomption favorise la pratique établie.

7. Évaluation I : Considérer les facteurs moraux et politiques affectés par la pratique en question. Quels pourraient être les préjudices, les menaces à l'autonomie et à la liberté ? Quels pourraient être les effets sur les structures de pouvoir, les implications pour la justice, l'équité, l'égalité, la hiérarchie sociale, la démocratie, etc.

8. Évaluation II : Demander comment le système ou les pratiques empiètent directement sur les valeurs, les buts et les objectifs du contexte. En outre, considérer la signification ou l'importance des facteurs moraux et politiques à la lumière des valeurs, des fins, des buts et des objectifs du contexte. En d'autres termes, que signifient les préjudices, les menaces à l'autonomie et à la liberté, ou les perturbations des structures de pouvoir et de la justice par rapport à ce contexte ?

9. Sur la base de ces résultats, l'intégrité contextuelle recommande ou ne recommande pas l'utilisation de la technologie ou de la pratique étudiée.

Dans la théorie de l'intégrité contextuelle de Nissenbaum, le niveau descriptif regroupe les étapes 1 à 6 de l'heuristique décisionnelle. Le niveau normatif comporte les étapes 7 et 8. Le niveau prescriptif correspond à l'étape 9.

Application de la théorie de l'intégrité contextuelle de Nissembaum

Le concept de « renseignement personnel »

Dans son livre de 2010, Nissenbaum explique en ces mots la visée de sa théorie de l'intégrité contextuelle : « understanding privacy expectations and the reasons that certain events cause moral indignation ». Elle s'intéresse aux « expectations about the flow of personal information » (p. 2) et elle retient comme définition de renseignement personnel « information about an identifiable person », c'est-à-dire « any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity » (p. 4).

Des écrits ultérieurs de Nissenbaum donnent à penser que cette définition des renseignements personnels devrait être élargie. Dns un article écrit avec S. Barocas en 2014, Nissenbaum affirme que :

> This is a subtle but crucially important point: insights drawn from big data can furnish additional facts about an individual (in excess of those that reside in the database) without any knowledge of their specific identity or any identifying information. Data mining breaks the basic intuition that identity is the greatest source of potential harm because it substitutes inference for using identifying information as a bridge to get at additional facts […] date collectors [can] draw inferences about precisely those qualities that have long seemed unknowable in the absence of identifying information (p. 55).
>
> Even when individuals are not 'identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis (p. 45).

Nous avons déjà souligné dans notre rapport précédent que l'analyse prédictive permet de *rapporter à une personne* des renseignements jugés intimes et sensibles et qui peuvent avoir un impact sur sa vie personnelle. La question même de l'identification comprise au sens strict (relier les renseignements de manière directe ou indirecte à l'identité civile de la personne, c'est-à-dire

à son nom, prénom, adresse, numéro d'assurance sociale, etc.) devient secondaire à l'ère de l'analyse prédictive. En quelque sorte, on peut « individualiser » et rejoindre une personne sur la base de renseignements intimes et sensibles sans nécessairement « l'identifier » (Poullet, 2020, p. 49). C'est pourquoi nous sommes d'avis que le concept de « renseignement personnel » devrait être élargi au-delà des risques d' « identification » et inclure les risques d' « individualisation ». D'ailleurs, Il est intéressant de noter que le Conseil de l'Europe, dans ses *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, précise que les données à caractère personnel réfèrent à « toute information concernant une personne physique identifiée ou identifiable (la personne concernée) » et ajoute que « les données à caractère personnel englobent également toute information utilisée pour individualiser ou singulariser des personnes identifiées sur la base d'informations relatives au profilage d'un groupe » (p. 3).

D'un point de vue descriptif : étapes 1 à 6 de l'heuristique décisionnelle

Ces dernières années, plusieurs chercheurs (Apthorpe, Varghese, et Feamster, 2019, Apthorpe, Shvartzshnaider, Mathur, Reinsman, et Feamster, 2018, Gerdon, Nissenbaum, Bach, Kreuter et Zins, 2021, Shvartzshnaider et al., 2016, Utz et al., 2021, Zhang et al., 2021; Zhang et al., 2022) se sont appuyés sur le cadre de l'intégrité contextuelle pour concevoir des enquêtes par vignette afin d'évaluer les effets des facteurs contextuels sur la perception des gens au regard du caractère approprié de différentes technologies : objets connectés, caméras de reconnaissance faciale, pratiques liées au virus du COVID-19, etc. Les vignettes proposées aux participants de ces enquêtes ont été générées en utilisant les paramètres clés de la théorie de l'intégrité contextuelle. Voici un exemple des paramètres utilisés pour les vignettes dans l'étude de Apthorpe, Shvartzshnaider, Mathur, Reinsman, et Feamster (2018) :

Table 1. CI parameter values chosen to generate smart home information flows. The *subject* parameter is not listed and was set to "its owner", referring to the owner and primary user of a device. We included a "null" transmission principle to generate unconditional information flows.

Sender	Recipient	Attribute	Transmission Principle
a sleep monitor	the local police	{subject}'s location	if {subject} has given consent
a security camera	government intelligence agencies	{subject}'s eating habits	if {subject} is notified
a door lock	{subject}'s doctor	the times {subject} is home	if the information is kept confidential
a thermostat	an Internet service provider	{subject}'s exercise routine	if the information is anonymous
a fitness tracker	its manufacturer	{subject}'s sleeping habits	if the information is used to perform
a refrigerator	other devices in the home	audio of {subject}	maintenance on the device
a power meter	{subject}'s immediate family	video of {subject}	if the information is used to provide
a personal assistant	{subject}'s social media accounts	{subject}'s heart rate	a price discount

Les études révèlent que les paramètres contextuels ont un impact significatif sur la perception des gens quant au caractère approprié ou inapproprié de l'utilisation des technologies axées sur les données. Ces études montrent que la variation ou l'omission de l'un des paramètres de la théorie de l'intégrité contextuelle a un effet direct sur la perception du caractère approprié. Ces recherches appuient l'idée que la théorie de l'intégrité contextuelle fournit un cadre d'analyse

utile pour démêler les attentes en matière de protection de la vie privée et contribue à une compréhension plus nuancée des enjeux en matière de vie privée. D'ailleurs, les chercheurs Zhang et al. concluent au terme de leur article de 2022:

> Our study illustrates how Context Integrity (CI) provides an effective framework for approaching controversial societal practices, such as VC deployment. It suggests that the multifactorial insights that CI yields can inform richer and more nuanced responses to challenges confronting society in today's fight against COVID-19, and potentially other similar challenges going forward. Our study shows that contextual parameters can significantly affect people's judgements about what is and isn't appropriate in the deployment of VCs.

Ces études s'inscrivent dans la lignée de la recherche « Measuring privacy: an empirical test using context to expose confounding variables » menée par Kirsten Martin et Helen Nissenbaum en 2015. Dans le cadre de leurs travaux, ces chercheures se sont intéressés aux renseignements jugés sensibles et ont reproduit l'enquête *Public Perceptions of Privacy and Security in the Post-Snowden Era* menée en 2014 par le Pew Research Center suivant une méthodologie traditionnelle (qui demande essentiellement aux gens d'identifier les renseignements jugés sensibles parmi ceux proposés) pour la comparer avec une méthodologie par vignettes où les paramètres clés sont modifiés. Chacun des 569 répondants devait évaluer 40 vignettes. Il est expliqué au terme de cet article que :

> For future surveys of privacy, this study reinforces the importance of how privacy is measured. Study designs should aim to disambiguate privacy rather than seek broad generalizations about consumers' privacy concerns. Past studies, including those that have been quite influential, have yielded cloudy and potentially misleading results, i.e., misleading information about how people understand and value privacy. This study exemplifies the importance of including confounding variables in the study of privacy—the context of an information exchange, how the information is used and transmitted, and the sender and receiver of the information all impact the privacy expectations of individuals.
>
> For public policy, this study suggests that relying on one dimension—sensitive information or not; privacy categorization of respondent—is limiting. Our study has called these concepts into question by showing 'sensitivity' of information and 'concern' about privacy are unstable in the face of confounding variables: privacy categories and sensitivity labels prove to be highly influenced by the context and use of the situation. In particular, focusing on differences in privacy expectations across consumers obscures the common vision of what is appropriate use of information for consumers (p. 214-215).

> The primary aim of this work is to call into question what useful inferences can be drawn from judgments of sensitivity and to influence the design of future such surveys so they take into account all parameters required to define information norms (p. 216).

La théorie de l'intégrité contextuelle semble donc offrir un cadre d'analyse efficace pour mesurer ce que les gens jugent approprié ou inapproprié au sujet de l'impact des nouvelles technologies sur le flux d'informations. Ce cadre se révèle utile pour mesurer, en tenant compte du contexte, l'acceptabilité sociale des nouvelles technologies ou des nouvelles pratiques en ce qui concerne le flux d'informations.

Notons cependant au passage une certaine confusion autour du concept de « principe de transmission ». Dans l'article de l'étude de Martin et Nissenbaum (2015) et dans l'étude de Zhang et al. (2021, 2022), le principe de transmission inclut l'utilisation, au sens de l'objectif ou de la fin, visée par le flux d'information. Pourtant, dans l'étude de Gerdon, Nissenbaum, Bach, Kreuter et Zins (2021) et dans le livre de Nissebmaumm (2010), le principe de transmission énonce seulement la condition appliquée au flux d'information (par exemple : le contrôle sur ses informations, la confidentialité, le consentement ou la réciprocité). Dans un séminaire en ligne de mars 2021, Nissenbaum explique que les récents développements numériques pourraient justifier le besoin d'ajouter un sixième paramètre, soit le « use parameter », qui contiendrait les finalités de l'utilisation. Nous pensons qu'il serait pertinent d'ajouter ce paramètre.

Nissenbaum explique que sa théorie de l'intégrité contextuelle permet de comprendre en quoi les inférences obtenues par analyse prédictive modifient les paramètres clés du flux d'information et engendrent ainsi un jugement *prima facie* en faveur d'une violation des normes informationnelles.

> The framework of contextual integrity allows us to assess the impact that these changes have had on information flows. Accordingly, when information subjects no longer share their metadata voluntarily, this affects the transmission principle. When the recipients of metadata have vastly increased capabilities of aggregating, storing, combining and analyzing metadata, this changes the attribute. And when we assume the risk of surveillance whenever we impart with information, this introduces a wider range of actors into the information flow. A careful analysis of these interdependencies also challenges the dichotomies courts have used to distinguish metadata from data, namely: content vs. non-content data, private records vs. business records held by third parties, and hard-to obtain information vs. information "in plain view." As we argue below, the fact that we no longer share information voluntarily undermines the notion that business records held by third parties deserve fewer privacy protections than private information held by the data subjects themselves. The fact that metadata is now aggregated, stored, combined and analyzed to enable a host of inferences (Kift et Nissenbaum 2017, p. 351).

Dans son article « The Origins of Personal Data and its Implications for Governance », Martin Abrams explique que les données « inférées » diffèrent des données « fournies » par l'individu et des données « observées », c'est-à-dire des données obtenues par l'observation de l'individu. À la différence de ces deux dernières sortes de données, les données « inférées » sont quant à elles créées à distance de l'individu et sans sa participation. Celui-ci n'est généralement pas conscient de la création de ces données le concernant.

En ce sens, l'analyse prédictive introduit un changement significatif dans le *principe de transmission*. En obtenant des données sur une personne à partir des données fournies par un grande nombre de personnes, l'analyse prédictive change l'*expéditeur*. Les données inférées peuvent être facilement partagées et utilisés par de tierces parties, ce qui a des incidences sur le *destinataire*.

Dans le cadre de leur recherche « Measuring privacy: an empirical test using context to expose confounding variables », Martin et Nissenbaum ont constaté que l'un des facteurs qui influencent le plus les attentes des personnes au regard de la vie privée est le fait que l'informations soit utilisée à des fins commerciales. À cet égard, certains contextes soulèvent des préoccupations particulières au regard des risques de discrimination, de manipulation des personnes ou d'inégalités sociales : le commerce par publicités personnalisées en ligne, les processus d'embauche, les assurances des personnes et le commerce par prix différenciés (*adaptive pricing*) selon le profil de l'acheteur internaute.

D'un point de vue évaluatif : étapes 7 et 8 de l'heuristique décisionnelle

Ainsi que nous l'avons expliqué, la description (étapes 1 à 6 de l'heuristique décisionnelle) n'est qu'un premier niveau d'analyse qui doit être suivi par une évaluation (étapes 7 et 8) lorsque la violation des normes informationnelles donne lieu à un jugement *prima facie*. Ce niveau introduit un ensemble de considérations plus générales sur les valeurs. En effet, Nissenbaum insiste sur le fait que la vie privée, en tant que flux d'information approprié, ne sert pas seulement les intérêts des personnes concernées, mais aussi « les valeurs, les fins et les objectifs spécifiques au contexte ». En ce sens, les valeurs occupent une place importante dans la théorie de l'intégrité contextuelle afin d'évaluer les utilisations appropriées ou inappropriées des nouvelles technologies qui affectent les flux d'informations. À cet égard, les professeurs Benyekhlef et Déziel formulent la remarque suivante :

> Il est intéressant de noter que Nissenbaum place, en un sens, la morale au-dessus du droit. Cette perspective nous semble assise sur une conception plus réaliste du droit, c'est-à-dire du droit envisagé comme une technologie sociale au service de la société, et, par le fait même, utilisée de façon à pourvoir à ses intérêts. Il importe donc de juger de la valeur morale du droit, d'évaluer ses effets en fonction de standards et de principes qui ne sont pas juridiques (2018, p. 46).

Le commissaire à la protection de la vie privée du Canada, M. Therrien, a d'ailleurs insisté sur l'importance des valeurs dans un régime de droit dans son message lors du dépôt du rapport au Parlement 2020-2021:

> Comme société, nous devons projeter nos valeurs dans nos lois sur le numérique. Une législation sensée devrait autoriser l'innovation responsable, qui est dans l'intérêt public et propre à susciter la confiance, mais interdire les utilisations de la technologie qui sont incompatibles avec nos droits et nos valeurs.

Le cadre théorique proposé par Nissenbaum fait appel aux valeurs, mais n'est pas très explicite sur la façon de procéder à l'évaluation de ces valeurs. Le niveau évaluatif de la théorie de Nissenbaum a été l'objet de critique. Notamment, le spécialiste Dennis Hirsch explique que :

> Contextual integrity theory does important work with respect to the regulation of predictive analytics. Rather than rely on the illusion of individual control, it draws a substantive line between data practices that are appropriate and those that are not. It further highlights existing informational norms as important points of reference for making this determination.
>
> But it is less helpful when it comes to deciding whether predictive analytics practices that break with social norms (which will likely be most such operations, given the newness of the field and the premium that it places on innovation) are nonetheless appropriate and acceptable. To determine whether such practices are acceptable, the theory would require one to assess whether the norm-breaking analytic practice is better able to promote "interests, general moral and political values, and context-specific ends, purposes, and values" such as "fairness, justice, freedom, autonomy, welfare, and others more specific to the context in question," than a norm-compliant one would be. This test is so vague as to be almost unworkable. Which general and context-specific interests and values is one to consider?

Soulevant des critiques similaires à celle de Hirsch, James B. Rule écrit que « Nissenbaum is merely proposing a framework for discussion, rather than a source of uniquely valid solutions to normative conflicts » (p. 272).

Force est de constater que le cadre évaluatif de Nissembaum ne permet pas d'identifier clairement les valeurs et les principes moraux qui doivent servir de standards éthiques pour l'évaluation des utilisations de données. Il ne contient pas d'indications sur la manière de mener l'évaluation éthique. Tel que présenté, ce cadre d'analyse demeure vague.

Il peut être pertinent de rappeler que l'évaluation dont il est question relève de l'éthique normative appliquée et qui porte sur le « devoir-être », c'est-à-dire sur ce qui devrait être fait. Il s'agit d'un champ de réflexion proposant des réponses argumentées à des questions éthiques, en

s'appuyant sur des méthodes et des théories élaborées principalement par des philosophes d'hier et d'aujourd'hui. Elle se distingue de l'éthique descriptive, qui consiste à décrire les enjeux éthiques et les valeurs en présence dans un contexte donné. Cette dernière rend compte des choix et des préférences des gens. En éthique normative, les critères et les raisons mis de l'avant pour juger les actions sont primordiaux. C'est en discutant de ces critères et de ces raisons qu'on peut parvenir à évaluer leur valeur et chercher à déterminer des règles de conduite justifiées. L'éthique normative tient compte des perceptions éthiques des gens mais vise, sur la base de la confrontation des points de vue, par la discussion et en se référant à des principes, à déterminer la meilleure action à envisager.

Au début de son livre de 2010, Nissenbaum affirme que « the framework of contextual integrity provides a rigorous, substantive account of factors determining when people will perceive new information technologies and systems as threats to privacy » (p. 2). Nous pouvons affirmer que cet objectif est atteint par la théorie de Nissenaum. Toutefois, le cadre normatif qu'elle propose n'est pas suffisant pour réaliser le deuxième aspect de l'objectif annoncé, soit : « it not only predicts how people will react to such systems but also formulates an approach to evaluating these systems and prescribing legitimate responses to them » (p. 2). Bien que la perspective proposée par Nissenbaum avec son cadre d'analyse semble pertinente, force est de constater que les outils proposés pour réaliser l'analyse éthique normative au regard des valeurs, des fins et des objectifs spécifiques au contexte doivent être développés.

Des outils d'analyse déjà existant en lien avec la vie privée et pourraient être employés pour compléter l'évaluation éthique pour la théorie de l'intégrité contextuelle. Parmi ces outils, il y a notamment le critère énoncé dans l'arrêt Oakes. D'ailleurs, dans son article « Privacy and the question of technology », la professeure à la Faculté de droit de l'Université de Toronto, Lisa Austin, avance que :

> This approach, which [Helen Nissenbaum] calls "contextual integrity," involves respecting the norms relating to information disclosure applicable to a particular context. I will argue that this approach is similar to, and compatible with, the "reasonable expectation of privacy" test as developed by the Supreme Court of Canada in the context of interpreting Canada's constitutional guarantee against unreasonable search and seizure (p. 129).

Dans son article de 2016, le professeur à la Faculté de droit de l'Université d'Ottawa Graham Mayeda insiste sur l'utilité du critère énoncé dans l'arrêt Oakes pour évaluer les limites de la protection de la vie privée :

> One way for the law to remain responsive to new contexts is to allow for a broad protection for privacy: limits should only be placed on it by law-makers or by courts after rigorous and nuanced consultation and consideration of the social meaning and value placed on the forms of social interaction that a particular form of privacy interest

> promotes and protects. In consequence, when a person alleges that their s 8 right has been infringed, the scope of privacy that underlies the protection in s 8 should be defined broadly. The balancing of competing rights should occur within the framework of s 1 and the application of the *Oakes* test, which allows for more nuanced, evidence-based balancing than the current s 8 test. Of course, this shift necessitates that the s 1 analysis be sufficiently robust to put the government to a meaningful test of justifying rights-infringing actions and laws.

Mayeda soutient qu'un nouveau paradigme de la vie privée est nécessaire pour le droit à la vie privée du Canada, soit un paradigme « that recognizes that the appropriate scope of privacy is highly contextual and *emerges* from new forms of social interaction, many ofwhich are mediated through new technologies or new uses of old technologies ». Ses préoccupations sur les contextes sociaux rejoignent celles de Nissenbaum. Mayeda ne fournit toutefois pas d'indications plus précises sur la façon d'appliquer, dans le cadre de ce nouveau paradigme, les principes mis de l'avant dans le critère énoncé dans l'arrêt Oakes. Rappelons que, à strictement parler, le critère énoncé dans l'arrêt Oakes s'applique seulement aux actes du gouvernement et non aux litiges entre parties privées et entre un individu et l'entreprise privée. Ce critère est utilisé lorsque le tribunal détermine qu'il y a eu violation de la *Charte*. Une certaine forme de protection du droit à la vie privée est offerte avec l'article 8 de la Charte, mais le droit à la vie privée ne figure pas en tant que tel parmi les droits et libertés qui y sont énoncés et protégés par la *Charte*.

Le Commissariat à la protection de la vie privée du Canada propose d'évaluer les impacts sur la vie privée en 4 questions[1]. Le critère en quatre parties proposé est une adaptation du critère de l'arrêt *Oakes*. Les quatre questions sont les suivantes :

1. Est-il démontré que la mesure est nécessaire pour répondre à un besoin précis?
2. Répondra-t-elle vraisemblablement efficacement à ce besoin?
3. La perte au chapitre de la vie privée serait-elle proportionnelle à l'avantage obtenu?
4. Existe-t-il un moyen moins envahissant d'arriver au même but?

Le principe de limitation de la collecte et le principe de nécessité sont consacrés par les lois de protection des renseignements personnels. Au Canada, le principe 4.4 de l'annexe 1 de la LPRPDE précise qu'une organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées. Au Québec, le critère de nécessité se retrouve notamment dans l'article 64 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et dans l'article 5 de la LPRPSP. La Commission d'accès à l'information du Québec (CAI) précise que le principe de nécessité est un « principe fondamental ayant pour objectif de réduire

[1] https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/

les atteintes à la vie privée des personnes concernées par les renseignements personnels recueillis par les entreprises privées et les organismes publics ».[2]

Le critère de « nécessité » a récemment été remis en question par des experts dans le contexte de l'intelligence artificielle et des technologies axées sur les données.

Dans son article « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives » de 2019, le professeur de droit Pierre-Luc Déziel explique que « le principe de limitation de la collecte ne pourra adéquatement encadrer les pratiques de collecte de renseignements personnels dans l'environnement numérique contemporain s'il ne s'en remet qu'au concept de nécessité […] les défis que pose l'intelligence artificielle et les données massives rendent ce concept largement inefficace et caduc » (p. 31). Le premier défi que posent l'intelligence artificielle et les données massives se retrouve sur le plan de la définition des fins qui sont visées par le traitement de l'information. À partir de la politique de l'utilisation des données de Facebook, le professeur Déziel explique que lorsqu'une fin d'expérience personnalisée est identifiée, tous les renseignements qui portent sur l'utilisateur peuvent a priori être justifiés comme étant nécessaires. Le principe de nécessité se trouve ainsi vidé de son sens. Le second défi que posent l'intelligence artificielle et les données massives pour les principes de limitation de la collecte et l'identification des fins concerne la délimitation des renseignements personnels qui pourront être qualifiés de nécessaires pour l'atteinte de ces fins. Dans le contexte de l'intelligence artificielle, les fins exactes ne pourront pas être clairement identifiées avant la fin du processus de traitement de l'information. Les finalités visées et la nécessité des données apparaissent qu'au terme de ce processus. « Le traitement de l'information dans le domaine de l'intelligence artificielle opère dans une perspective temporelle qui bouscule les fondements traditionnels du droit à la vie privée » (p. 23).

D'ailleurs, la Commission de l'éthique en science et en technologie (CEST) propose également de penser la protection du critère de nécessité dans le contexte de l'analyse prédictive et des données massives :

> Au-delà du respect du critère de nécessité de la collecte, les données utilisées devraient, pour ainsi dire, faire l'objet d'une attention au regard de la légitimité de la finalité de leur traitement […] Par conséquent, il serait opportun que le projet de loi assure une protection des renseignements inférés, particulièrement pour ceux qui ont un caractère sensible de par le haut degré d'attente raisonnable en matière de vie privée qu'auraient les individus concernés par ces renseignements, ou de par les conséquences potentielles de leur utilisation sur l'autonomie, la dignité ou l'intégrité de la personne. De manière concrète, la loi pourrait définir certains types de savoirs, à haut degré de sensibilité, qu'il

[2] https://www.cai.gouv.qc.ca/la-collecte-de-renseignements-personnels/

> est interdit d'inférer à partir de renseignements collectés ou partagés (CEST, 2020, p. 14 et 12).

Solove et Citron rappellent pour leur part que :

> Legal intervention should be designed to ensure that socially beneficial information practices continue. Our economy depends upon the collection and sharing of personal data. At the same time, personal data practices are inherently risky. Privacy law aims to ensure that personal data is used properly, that individuals have the ability to make decisions about their personal data, that there are meaningful guardrails and boundaries about how data is collected, used, or disclosed (Solove et Citron 2021).

Le professeur Déziel précise que le concept de nécessité demeure toutefois pertinent et efficace dans des contextes où des techniques d'intelligence artificielle et la collecte massive de données n'interviennent pas.

En se référant à l'interprétation du critère de l'arrêt Oakes par le juge Fillion de la Cour du Québec dans l'affaire *Société de Transport de la Ville de Laval c. X*, le professeur Déziel insiste sur la pertinence du critère de l'arrêt Oakes dans le cadre d'une analyse des modes d'encadrement des pratiques de collecte de renseignements personnels en fonction des fins raisonnables à l'ère des technologies axées sur les données. Nous sommes aussi d'avis que le caractère important et légitime des fins, l'existence d'un lien rationnel entre les fins visées et la collecte et la nature des renseignements collectés et le principe de proportionnalité demeurent pertinents pour une évaluation éthique des technologies axées sur les données dans le cadre d'une approche comme celle proposée par Nissenbaum. Ces éléments mériteraient d'être approfondis en lien avec cette approche.

La protection de la vie privée des groupes d'individus

Jusqu'à maintenant, il a été question de la protection de la vie privée des individus. La plupart des juridictions protègent d'ailleurs la vie privée dans une perspective individuelle. Plusieurs spécialistes soutiennent qu'il est nécessaire d'élargir cette perspective à l'ère de l'analyse prédictive. C. Villani réfère à ces préoccupations dans son rapport *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne* :

> Le développement de l'IA fait apparaître un certain nombre d'angles morts dans la législation actuelle – et future avec le RGPD – en matière de protection des individus. Ceux-ci découlent du fait que la loi Informatique et Libertés, comme le RGPD, ne traitent que des données à caractère personnel. Or, si la portée des protections offertes par ces textes est potentiellement très large, l'intelligence artificielle ne mobilise pas uniquement des données personnelles. Loin s'en faut : beaucoup de ces enjeux soulevés par les algorithmes constituent aujourd'hui un angle mort du droit.

> En effet, la législation sur la protection des données n'encadre les algorithmes d'intelligence artificielle que dans la mesure où ils se fondent sur des données à caractère personnel et où leurs résultats s'appliquent directement à des personnes. C'est le cas d'un bon nombre d'entre eux : offres personnalisées, recommandations de contenus,… mais, de fait, beaucoup d'usages échappent à cette législation, bien qu'ils recèlent des **effets significatifs sur des groupes d'individus**, et donc sur les personnes. Il a par exemple pu être démontré que les agrégats statistiques qui ont pu motiver d'envoyer des patrouilles de police ou des livreurs Amazon plus souvent dans tel ou tel quartier peuvent alimenter des effets discriminants sur certaines catégories de population, par un mécanisme de reproduction des phénomènes sociaux (2018, p. 140. C'est nous qui soulignons).

P. Mavriki and M. Karyda expliquent que « researchers suggest that, since most people are not targeted by profiling and machine learning technologies as individuals, but as members of specific groups, the privacy of these groups needs to be examined further and considered in the context of data protection » (2019, p. 184).

Les chercheurs en question sont les défenseurs d'une conception distinctive de la vie privée nommée « *group privacy* ». Ils ont fait paraître en 2017 l'ouvrage collectif *Group Privacy: New Challenges of Data Technologies* édité par L. Taylor, L. Floridi et B. van der Sloot. Le concept de « groupe » auquel ces chercheurs renvoient n'est pas le groupe comme on l'entend de manière générale, c'est-à-dire des personnes qui se réunissent en référence à des intérêts communs. Il s'agit de groupes de personnes qui partagent une identité générique générée au moyen d'algorithmes sur la base de l'analyse de données massives. Il s'agit ainsi de groupes algorithmiques. Les renseignements obtenus à propos du groupe algorithmique ne sont pas simplement applicables aux personnes qui composaient l'échantillon initial, mais généralisables et transposables à l'ensemble des personnes qui partagent les mêmes caractéristiques que celles de la population de base. Ainsi, ces renseignements émergents peuvent être applicables à des personnes dont les renseignements ne furent pas initialement partagés ou analysés, ce qui soulève des préoccupations quant à leur vie privée.

Dans l'introduction de leur ouvrage *Group Privacy: New Challenges of Data Technologies*, les éditeurs L. Taylor, L. Floridi et B. van der Sloot expliquent :

> Although specific individuals may be harmed or benefited by certain data uses, this again is increasingly incidental in the big data era. Policies and decisions are made on the basis of profiles and patterns and as such negatively or positively affect groups or categories. This is why it has been suggested that the focus should be on group interests (2017, p. 14-15).

Selon eux, « a full understanding of group privacy will be required to ensure that our ethical and legal thinking can address the challenges of our time » (2017, p. 22). Ils affirment que : « as algorithmic societies develop, attention to group privacy will have to increase if we wish to avoid abuses and misuses » (2017, p. 21).

En quelque sorte, selon les défenseurs de la conception distinctive de la vie privée nommée « group privacy », la possibilité d'établir des inférences ne pose pas seulement des risques pour les individus, mais également pour les groupes qui, s'ils ne sont pas suffisamment protégés, sont vulnérables à la discrimination et à la manipulation. En plus de menacer les libertés de chaque individu pris séparément, l'analyse prédictive introduit ainsi des risques de discrimination pour des groupes d'individus en tant que groupe sur la base d'attributs inférés par corrélations (par exemple, les personnes homosexuelles, les personnes de telle idéologie politique, les personnes avec telle habitude de vie, etc.). Selon ces spécialistes, le concept de « *group privacy* » doit être pris en considération dans l'élaboration de mesures de protection de la vie privée.

Nous sommes d'avis que les défenseurs de la conception distinctive de la vie privée nommée *« group privacy* » ont mis en lumière un angle mort du droit et que la protection de la vie privée, à l'ère de l'analyse prédictive, doit prendre en considération les risques que soulèvent le traitement de données massives pour les groupes d'individus. Toutefois, la question est alors de déterminer le type de protection à apporter. Il a été suggéré d'élargir le concept de « renseignement personnel » pour y inclure non seulement les renseignements concernant des individus, mais aussi à propos de groupes algorithmiques. Il est avancé que les groupes algorithmiques devraient bénéficier d'un droit à la vie privée en tant que groupe.

Nous pensons que c'est une chose de reconnaître l'impact du traitement de données pour un groupe d'individus, et c'est une autre chose de créer un droit à la vie privée pour ce groupe en tant que groupe algorithmique. Il nous semble que, d'un point de vue ontologique, le concept de « groupe algorithmique » dont il est question ne va pas de soi. Ce sont des groupes qui n'existaient pas auparavant dans la société et qui sont générés par l'exploration de données agrégées. Les personnes concernées par le groupe n'ont pas connaissance de l'identité des autres membres du groupe, n'ont aucune relation avec eux et ont une perception limitée de leurs problèmes collectifs. En outre, ces groupes ont une géométrie variable et les individus peuvent passer d'un groupe à l'autre selon les analyses réalisées. Les groupes algorithmiques diffèrent des groupes auxquels des droits ont attribués (*groups rights*) dans le passé. Il n'est pas évident pour l'instant qu'un statut juridique peut être reconnu pour ces groupes.

Surtout, nous pensons que les intérêts de ces groupes algorithmiques peuvent être protégés autrement. Nous avons proposé l'adoption de mesures de protection législatives qui encadrent l'utilisation des renseignements inférés, en plus des mesures déjà mises en place pour la collecte. Nous pensons qu'un encadrement des usages inacceptables en amont permettrait de protéger autant les individus que les groupes d'individus des risques de préjudices que soulève l'analyse

prédictive. C'est d'ailleurs la suggestion avancée par des auteurs de l'ouvrage *Group Privacy: New Challenges of Data Technologies* :

> How, then, can we envisage the protection of "passive" groups extracted by the data analysis process ? In the impossibility of granting them sovereignty over or a right to control group data, their protection should focus on a different point in the chain of data collection, analysis, and targeting. Where a group cannot be given control over its data (because there is no structured group with capacity to exercise that control), the goal should be to protect the group's essential interests – primarily, its safety – at the analysis and targeting stages, by anticipating and regulating the riskiest uses of data. Where there is no legal subject to benefit from a privacy right, one solution may be to simply guard against harmful abuses of available data by other stakeholders.

Ainsi, l'approche par les risques (*risk-based approach*) nous semble un bon moyen d'offrir une protection aux groupes algorithmiques en incluant parmi les possibles préjudices ceux qui touchent ces groupes. Il s'agit d'élargir l'éventail des intérêts à sauvegarder au-delà du périmètre traditionnel au sein de l'approche par les risques. D'ailleurs, la réglementation en matière de protection des données met de plus en plus l'accent sur l'évaluation des risques, ainsi que le souligne A. Mantelero dans son rapport qui a mené aux *Lignes directrices sur l'intelligence artificielle et la protection des données* du Conseil de l'Europe adoptées en 2019. Le règlement de l'Union européenne sur l'IA (*Artificial Intelligence Act*) proposé en avril 2021 introduit une distinction entre les utilisations de l'IA qui créent un risque inacceptable, un risque élevé et un risque faible ou minimal. Notamment, il est affirmé que les pratiques de manipulation, d'exploitation et de contrôle social constituent des risques inacceptables et devraient être interdites « car elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit, et elles portent atteinte aux droits fondamentaux de l'Union » (p. 24).

L'idée de prédire les répercussions potentielles de l'intelligence artificielle sur le droit à la vie privée des personnes au regard des risques se retrouve dans d'autres régulations. Mentionnons aussi au passage la *Directive sur la prise de décision automatisée* adoptée par le gouvernement du Canada et qui est entrée en vigueur le 1er avril 2019. La Directive a comme principal objectif de s'assurer que les systèmes décisionnels automatisés soient utilisés de manière à réduire les risques qu'ils représentent pour les droits, la santé et le bien-être des personnes et des collectivités.

Préjudices qui relèvent de la protection de la vie privée et autres préjudices

Les défenseurs d'une conception distinctive de la vie privée nommée « *group privacy* » associent protection de la discrimination et protection de la vie privée. En affirmant que la vie privée

consiste en un flux d'information approprié, le cadre théorique de Nissenbaum est ouvert à la possibilité de protéger la discrimination au moyen de mesures de protection sur la vie privée. La discrimination est toutefois un enjeu qui dépasse largement la protection de la vie privée et qui peut être considéré comme un risque distinct de ceux qui concernent la vie privée. Dans quelle mesure revient-il aux mesures de protection de la vie privée de prendre en charge les risques de discrimination ?

Nissenbaum n'est pas explicite à ce sujet dans son livre de 2010. Dans un article publié en 2014, elle laisse sous-entendre qu'il existe un lien entre protéger une personne de la discrimination et protéger la vie privée.

> Take, for example, an applicant who is denied admission to college based on predictive analytics performed on a dataset aggregated from diverse sources, including many that have not traditionally featured into admissions decisions. Imagine further that these additional sources allowed the college to discriminate – perhaps unwittingly – against applicants on the basis of criteria that happen to correlate with socioeconomic status and thus with the likely need for financial aid.[16] While the outcome of such decisions may be judged unfair for many reasons worth discussing, it is the role of privacy – the role of disruptive informational flow – that we wish to note in this case […]
>
> Why, one may ask, insist on the centrality of privacy? First, doing so deepens our understanding of privacy and its instrumental value and at the same time highlights the distinctive ways that other ethical values are impinged and sustained, specifically, by the ways information does and does not flow. Privacy is important, in part, because it implicates these other values. Second, doing so also allows us to better formulate interventions, regulations, or remediation for the sake of these values. By keeping in view connections with specific information flows, certain options become salient that might otherwise not have been. Parsing cases in which big data gives rise to discrimination in terms of contextual integrity forces us to be much more specific about the source of that unfairness because it compels us to account for the disruption that made such discrimination possible (Barocas et Nissenbaum, 2014, p. 48-49).

Il est intéressant de noter ici que Nissenbaum insiste sur la valeur instrumentale de la protection de la vie privée. Cette protection est perçue ici comme un moyen pour la protection d'autres valeurs. Le professeur Déziel insiste sur cette distinction :

> Les auteurs présentés dans cette section perçoivent la protection de la vie privée comme une *fin* en soi, c'est-à-dire comme quelque chose qui possède une valeur intrinsèque, ou comme un *moyen*, c'est-à-dire un véhicule permettant l'atteinte d'autres objectifs qui sont aussi désirables. Évidemment, ces deux points de vue ne sont pas concurrents et se complètent. Voir la vie privée comme une fin en soi *et* comme un moyen dans la poursuite d'autres intérêts n'est pas contradictoire, au contraire. La protection de la vie

> privée, au-delà des avantages qu'elle entraîne sur les plans politiques et sociaux, est une condition nécessaire au respect de la dignité et de l'autonomie de la personne. C'est la raison pour laquelle, nous semble-t-il, les atteintes à la vie privée peuvent être sanctionnées même si elles n'ont pas entraîné de préjudices ou de dommages particuliers à la personne. En droit canadien, le simple fait de porter atteinte à la vie privée de la personne *est* une faute. La victime n'a pas à démontrer quelles conséquences négatives furent engendrées par la violation de sa vie privée. Ainsi, force est d'admettre que le droit canadien voit la protection de la vie privée non pas comme un simple moyen, mais comme une fin en soi (p.64).

Il n'est toutefois pas clair si la protection de la vie privée a aussi pour NIssenbaum une valeur en soi, si elle peut être considérée comme une fin.

Y a-t-il des préjudices qui relèvent de la vie privée en tant que telle? La professeure de droit Lisa Austin le pense. Elle donne en exemple la surveillance :

> There is a deeper intuition that we have about privacy, however, that I do not think is captured by this sense of privacy as a protection from other kinds of wrongs. In some situations, we want to say that privacy is something that we lose and that this loss can itself be a wrong. Depending on our theory of privacy, we will identify losses of privacy differently. However, one case about which there is considerable agreement is that of surveillance. Being placed under the public gaze, such as in the case of widespread surveillance, results in a loss of privacy.

Selon elle, nous pouvons être inhibés dans nos expressions et nos actions lorsque nous prévoyons qu'elles susciteront des réactions désagréables de la part d'autrui, même si ces réactions ne constituent pas des torts indépendants tels que le harcèlement et la discrimination. En ce sens, la vie privée protège notre capacité à agir et à penser de manière différente ; elle protège l'individualité.

> La personne qui est contrainte de vivre chaque minute de sa vie parmi les autres et dont chaque besoin, pensée, désir, fantaisie ou gratification est soumis à l'examen public, a été privée de son individualité et de sa dignité humaine. Un tel individu se fond dans la masse (Edward J. Bloustein, 1962, p. 962).

Mentionnons au passage l'idée de Thomas Nagel selon laquelle l'expression d'émotions fortes (par exemple, l'expression de la tristesse ou de la colère) est par essence incompatible avec le fait d'afficher un visage en public. Certains aspects de notre vie intérieure, et de nos relations intimes, ne peuvent tout simplement pas exister s'ils sont exposés au regard du public, même s'ils sont, d'une certaine manière, tout à fait conventionnels. L'analyse de Nagel se concentre sur la vie émotionnelle. Nous pouvons également établir des parallèles avec nos pensées. Il suffit de se référer aux différences entre le fait de réfléchir à quelque chose pour vous-même, d'en discuter

avec un ami, de présenter une communication à des collègues et de prononcer une conférence devant une foule nombreuse. Nous ressentons de la pression même si nous disons quelque chose de tout à fait conventionnel.

Bien qu'il reconnaisse que les préjudices liés à la manipulation sont distincts des atteintes à la vie privée, le spécialiste américain Hirsch (2020) pense la protection de la vie privée doit être élaborée en pensant aux risques de manipulation rendues possibles par l'utilisation de renseignements inférés. En effet, les données personnelles et intimes, inférées par analyse prédictive, sont dans certains cas la condition même de la manipulation. En encadrant la production de ces renseignements inférés, il serait possible de limiter les risques de manipulation et ainsi de protéger les personnes.

C'est également l'avis de Matz, Appel et Kosinski. Dans leur article « Privacy in the age of psychological targeting » (2020), ces auteurs définissent ainsi le ciblage psychologique (*psychological targeting*) :

> Le ciblage psychologique est la pratique qui consiste à extraire les profils psychologiques des personnes à partir de leurs empreintes numériques (par exemple, leurs *likes* Facebook, leurs *tweets* ou leurs enregistrements de cartes de crédit) afin d'influencer leurs attitudes, leurs émotions ou leurs comportements par le biais d'interventions psychologiques à grande échelle.

Ces chercheurs expliquent que l'efficacité du ciblage psychologique est directement liée au fait que le message soir adapté aux caractéristiques personnelles de la personne sur la base des inférences générées sur la personne. Pour ces chercheurs :

> [P]olicy makers should consider regulation that directly addresses psychological targeting, for example, by restricting its use in specific contexts such as political campaigning and establishing clear standards for algorithmic fairness that prevent discrimination. Importantly, regulators have to take into account that seemingly innocuous data can be transformed into private traits and states. They should go beyond protecting specific data types from isolated areas, like health care and credit card data, and instead develop protection of data at all levels (including metadata) with a focus on which insights might be inferred from them (p. 118-119).

Solove est d'avis qu'il revient aux lois de protection de la vie privée de réglementer le flux d'informations personnelles :

> Losing control over our personal data constitutes an injury to our peace of mind and our ability to manage risk. In the clutches of organizations, personal data can be used for a wide array of purposes for an indefinite period of time. Privacy laws seek to regulate data flows to protect individuals from potential downstream uses.

Il insiste d'ailleurs sur la possibilité de restreindre le flux d'information :

> Some argue that it is impossible for the law to limit how others use our data, but this is false. Copyright law is a clear example of the law regulating the way information is used and providing control over that data. I am not suggesting that copyright law is the answer to privacy, but it illustrates that it is possible for the law to restrict uses of data if it wants to. We can protect privacy, even in light of all the collection, dissemination, and use of our information. And it is something we must do if we want to protect our freedom and intellectual activity in the future.

Le professeur de droit à l'Université McGill, Ignacio Cofone, explique dans son article « Antidiscriminatory privacy » que les règles de protection de la vie privée devraient, s'ils le peuvent, servir à prévenir des préjudices de la discrimination, notamment en identifiant et bloquant les points de données qui sont considérées comme des substituts des catégories que la loi veut protéger. Cofone est d'avis que la protection de la vie privée doit protéger plus largement les intérêts sociétaux.

La professeure Austin pense aussi que la protection de la vie privée peut et doit jouer un rôle instrumental en protégeant des intérêts qui ne relèvent pas nécessairement de la vie privée : « I think that it is unfortunate that regulatory regimes such as PIPEDA do not embrace a range of interests beyond privacy » (. 166). Elle présente d'ailleurs ces exemples :

- Un gouvernement qui utiliserait les informations recueillies sur les personnes pour éliminer les dissidents. Le meilleur remède contre cela est d'empêcher la collecte d'informations en premier lieu. Dans cette optique, la vie privée peut être comprise comme un droit qui limite la capacité du gouvernement à collecter certains types d'informations sur un individu comme les opinions politiques et l'appartenance religieuse.

- Il existe certaines informations sur nous-mêmes qui, si elles étaient connues des autres, nous rendraient vulnérables au harcèlement, à la discrimination ou à d'autres types d'abus. Par exemple, une préoccupation émergente est celle du vol d'identité, par lequel un individu acquiert des éléments clés de l'identité d'une autre personne (tels que le nom, l'adresse, le numéro de téléphone, le numéro d'assurance sociale, le numéro de permis de conduire, les informations relatives aux cartes de crédit et aux comptes bancaires, les certificats de naissance et les passeports) puis les utilise pour se faire passer pour cette personne et se livrer à diverses pratiques frauduleuses.

Toutefois, précise la professeure Austin, il faut éviter de confondre les préjudices qui relèvent spécifiquement de la vie privée et les préjudices qui ne tombent pas sous la rubrique « vie privée », mais pour lesquelles la protection de la vie privée fonctionne comme une protection anticipée (*anticipatory remedy*). Par exemple, si la séropositivité d'une personne est considérée comme privée afin d'assurer une certaine protection contre la discrimination, le préjudice en

question est la *discrimination* qui en résulte et non *l'atteinte à la vie privée*. Mais au lieu d'attendre qu'une telle discrimination se produise et d'y remédier, nous pourrions vouloir prévenir la discrimination en premier lieu. Accorder un droit à la vie privée sur son statut VIH peut ainsi fonctionner comme une sorte de réparation anticipée (*anticipatory remedy*).

Il est également important de reconnaître que ces torts peuvent être protégés indépendamment de la protection de la vie privée. Il s'agit en quelque sorte d'évaluer si la protection de la vie privée est la protection anticipée la plus efficace et si le préjudice en question pourrait être empêché autrement. Par exemple, avec la *Loi sur la non-discrimination génétique* (L. C. 2017, ch. 3), il a été décidé de protéger les renseignements génétiques dans le cadre d'une loi dont l'objectif est de combattre la discrimination.

Or cette distinction concernant les types de préjudices (ceux qui relèvent de la vie privée et ceux n'en relèvent pas) ne semble pas clairement établie pour la théorie de Nissenbaum et la typologie des *privacy harms* de Solove et Citron dont nous parlerons dans un instant. Il y aurait lieu de mener un travail de clarification à cet égard. Nous pensons que la distinction proposée par Austin est porteuse et mériterait qu'on s'y attarde.

La dimension sociale de la protection de la vie privée et la théorie de l'intégrité contextuelle

Alors que la protection de la vie privée a été principalement défendue en fonction de ses avantages pour l'individu au cours du 20e siècle, une abondante littérature a mis de l'avant au cours du 21e siècle la dimension sociale de la protection de la vie privée, en plus des enjeux pour les groupes d'individus soulignés par les défenseurs d'une conception distinctive de la vie privée nommée « *group privacy* ». Les auteurs de l'anthologie *Social Dimension of Privacy* publiée en 2015 soutiennent que la reconnaissance des dimensions collectives de la vie privée doit jouer un rôle central dans la façon dont nous comprenons la vie privée et dont nous abordons les controverses actuelles sur la vie privée. Solove explique que :

> Privacy is not something that atomistic individuals possess in the state of nature and sacrifice in order to join the social compact. We establish privacy protections because of their profound effects on the structure of power and freedom within society as a whole. The protection of privacy shields us from disruptions to activities important to both individuals and society. (Solove, 2008).

Nous sommes en accord avec le professeur de droit A. Mantelero (2016) quant aux bénéfices engendrés par le cadre réglementaire régulant le traitement des données personnelles :

> Both privacy and data protection play an important role in safeguarding not only individual interests, but also the quality of society in general. Freedom of association,

> limits to disproportionate surveillance practices, and prevention of discrimination based on sensitive personal data are just few examples of the social effects of safeguarding the right to privacy and personal information. Values such as democracy and pluralism are strictly related to the protection of these rights (p. 245).

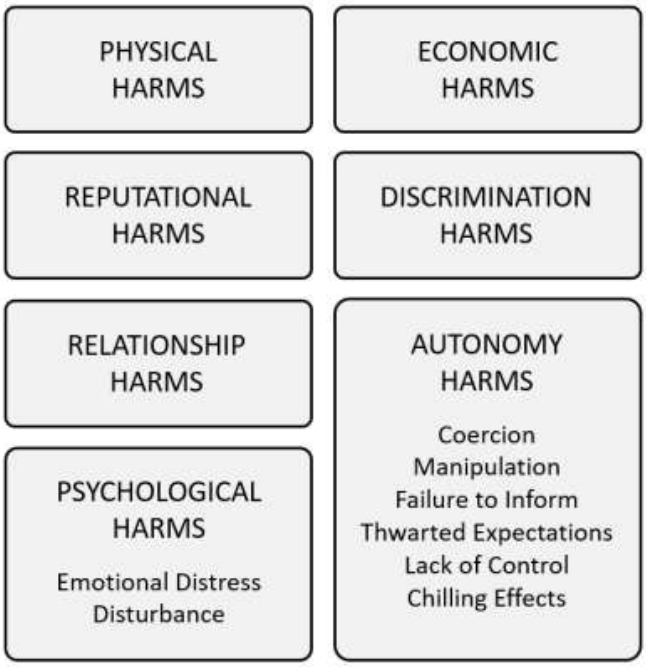
Le professeur Cofone avance avec raison qu' « au-delà des risques individuels, le traitement de renseignements personnels pose des risques sociaux, ce qui renvoie à l'idée que la protection de la vie privée est un droit de la personne » (2020).

Dans son livre de 2019, Yves Poullet explique à juste titre que le droit à la vie privée est doublement fondamental : « fondamental, car il représente la garantie de l'épanouissement personnel, fondamental également dans la mesure où il conditionne l'exercice de l'ensemble des autres libertés et droits fondamentaux » (p. 80).

En mettant l'accent sur les normes sociales, Nissenbaum reconnaît que les dimensions collectives doivent jouer un rôle central dans la façon dont nous comprenons la vie privée. Selon sa théorie, une attaque contre la vie privée individuelle est une attaque contre le tissu même de la vie sociale et politique : « As troubled as we might be by technologies that diminish control over information about ourselves, even more deeply troubling are those that disregard entrenched norms because, as such, they threaten disruption to the very fabric of social life » (2010, p.3). Il importe de préserver les interactions sociales importantes pour les individus, les groupes d'individus et la société. En décrivant la vie privée comme le flux approprié d'informations personnelles, la théorie de Nissenbaum a l'avantage de tenir compte des risques tout autant que les avantages que représentent les inférences algorithmiques pour les individus de l'ensemble de la société. Elle permet une forme d'autonomie interactive et relationnelle suivant laquelle la personne gère ses données, mais est intégrée dans une collectivité qui met en œuvre une certaine forme de protection collective susceptible d'évolution et qui la protège. Nous sommes d'avis qu'une réflexion sur l'impact des inférences algorithmiques ne devrait pas se limiter aux effets négatifs de ces inférences, mais devrait également prendre en considération les effets potentiellement positifs de celles-ci et ainsi faciliter certaines utilisations de renseignements inférés. En santé, par exemple, l'analyse prédictive peut contribuer à la recherche médicale et améliorer certains traitements. Elle offre un point d'équilibre entre la maximisation des libertés individuelles et les composantes d'un réseau d'informations utile ou nuisible à l'intérêt général.

Par ailleurs, nous pensons que l'application du cadre théorique de Nissenbaum afin de juger de l'impact de nouvelles technologies, en particulier l'étape 7 de son heuristique décisionnelle qui porte sur les préjudices (*harms*), bénéficierait des nombreux travaux menés ces dernières années par différents spécialistes au sujet des préjudices à la vie privée (*privacy harms*), et en particulier la typologie qui vient d'être publiée par D. Solove et D. Citron. Une analyse plus détaillée des préjudices faciliterait, il nous semble, l'dentification des valeurs et des principes éthiques, identification qui a été ciblée comme une faiblesse de la théorie de Nissenbaum. La typologie se veut une mise à jour des 4 atteintes à la vie privée identifiées par William Prosser dans les années

60 et prend en considération les distinctions avancées récemment par les autres spécialistes. Elle se présente ainsi :



Cette typologie a l'avantage de prendre en considération les risques pour les individus et les groupes d'individus ainsi que les avantages de la protection de la vie privée pour la société. Mais cette typologie n'est pas sans soulever des questions. Ne laisse-t-elle pas ouverte la question d'identifier les préjudices qui relèvent de la protection de la vie privée informationnelle et ceux qui devraient être protégés autrement que par des lois dont l'objet est la protection de la vie privée ? Solove et Citron ne fournissent pas de précisions à cet égard dans leur article. Le manque de contrôle (« lack of control ») n'est-il pas un préjudice qui en recoupe d'autres, notamment la manipulation ? Y a-t-il des risques que Solove et Citron ont négligé et qui ont été mis en lumière par d'autres spécialistes de la question, notamment M. R. Calo (« The Boundaries of Privacy Harm »), I. N. Cofone (« Privacy Harms »), K. Crawford et J. Schultz (« Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms ») et D. Hirsch (« From Individual Control to Social Protection: New Paradigms for Privacy Law In The Age of Predictive Analytics » ? Il est besoin de poursuivre l'analyse des préjudices, amorcée récemment par des spécialistes, dans le cadre d'une approche fondée sur les risques.

Conclusion

Étant donné les défis que posent les technologies axées sur les données— en particulier l'analyse prédictive—aux lois et aux principes actuels de protection des renseignements personnels, nous avons avancé l'idée qu'il est nécessaire d'adopter des mesures législatives qui encadrent

l'*utilisation* des renseignements inférés en plus des mesures mises en place concernant les pratiques de *collecte*. Nous pensons qu'un encadrement des usages inacceptables en amont permettrait de protéger davantage les personnes des risques de préjudices que soulève l'analyse prédictive et de pallier ainsi les limites des cadres de protection existants. Le présent rapport a été l'occasion d'approfondir cette proposition. Dans cette conclusion, nous mettrons en évidence les principales idées présentées dans le présent rapport sur la base des considérations du premier rapport. D'abord, nous rappellerons brièvement les principaux défis que pose l'analyse prédictive aux cadres réglementaires actuels. Ensuite, nous mentionnerons les principaux éléments que devrait prendre en considération, selon nous, l'analyse des risques de préjudices : le risque d' « individualisation » en plus du risque d' « identification »; les risques pour les groupes d'individus en plus des risques individuels ; les avantages collectifs de la protection de la vie privée. Nous expliquerons que la théorie de l'intégrité contextuelle proposée par Helen Nissenbaum est un cadre théorique pertinent pour l'analyse des risques de préjudices, s'il est notamment complété par les travaux récents de spécialistes qui ont mis en lumière la nature des préjudices pour la vie privée des personnes qui découlent de l'analyse prédictive (*privacy predictive harms*). En terminant, nous dirons quelques mots sur les travaux à venir.

Les technologies axées sur les données, en particulier l'analyse prédictive, sont maintenant utilisées pour inférer des attributs personnels et pour prédire le comportement humain à partir de vastes quantités de données issues de sources variées, notamment des données produites en continu sur Internet. Plusieurs recherches démontrent en effet que les outils d'analyse prédictive peuvent servir à inférer des renseignements considérés privés et sensibles à partir de données qui sont anodines lorsque prises isolément, mais qui, par regroupement avec d'autres données, révèlent les opinions politiques, les croyances religieuses, l'orientation sexuelle, le mode de vie, l'état de santé ou les traits de personnalité. Ces renseignements sur un individu sont *générés* par des personnes ou par des organisations à partir d'informations qui, en elles-mêmes, sont insignifiantes et ne soulèvent pas d'enjeux de vie privée. L'analyse prédictive introduit un nouveau mode d'acquisition des renseignements sur les personnes. Bien que les renseignements inférés puissent être employés à des fins relativement banales, il existe toutefois des risques de biais, de profilage, de discrimination et de manipulation des opinions ou des comportements qu'engendre cette connaissance émergente et un contrôle peut être exercé sur la vie des personnes.

L'avènement de l'analyse prédictive constitue un véritable défi pour l'application de certains principes traditionnels et règles de protection des renseignements personnels.

En effet, les cadres actuels de protection de la vie privée sont essentiellement basés sur le paradigme du contrôle individuel. Ils consistent à fournir aux individus des mesures leur permettant de contrôler la collecte, l'utilisation et la communication de leurs renseignements personnels, notamment au moyen du consentement. Or, dans le contexte de l'analyse prédictive et des données massives, il devient de plus en plus difficile, voire même impossible, pour un individu de contrôler efficacement les renseignements personnels le concernant et de se protéger par lui-même contre les préjudices découlant de l'analyse prédictive. L'enjeu avec ces

technologies n'est pas tant le partage ou l'utilisation de renseignements privés détenus par un individu, mais les renseignements privés générés à distance de l'individu et souvent à son insu à partir d'une énorme quantité de données provenant de sources variées. Afin de protéger les personnes des risques découlant de l'analyse prédictive, avons-nous expliqué, il ne suffirait pas de seulement ajouter la notion d' « inférences » dans les éléments de la définition de « renseignement personnel » des cadres de protection actuels basés sur le paradigme du contrôle individuel.

Par ailleurs, le principe de limitation de la collecte et le principe de nécessité, consacrés par les lois de protection des renseignements personnels, sont mis au défi par les technologies axées sur les données. Le fonctionnement de ces technologies repose en effet sur des corrélations par définition non prévisibles, mais significatives, parmi les données les plus diverses et riches possibles. Dans la mesure où les finalités visées et la nécessité des données apparaissent alors qu'au terme du processus de traitement des données, le principe de limitation de la collecte et le principe de nécessité ne peuvent encadrer adéquatement les pratiques de collecte de renseignements personnels dans le contexte des technologies axées sur les données. En quelque sorte, l'application stricte de ces principes va à l'encontre même du fonctionnement de l'analyse prédictive (Poullet, 2021). Cette application aurait d'ailleurs pour effet d'empêcher les résultats bénéfiques qui peuvent découler de l'utilisation de cette technologie et des données massives, notamment en recherche et dans le domaine de la santé. Ainsi que le souligne J. Cohen, « respect for privacy does not require absolute secrecy for personal matters. Rather, it entails something easier to imagine but more difficult to achieve : more openness about some things and less openness about others » (2012).

Traditionnellement, l'anonymisation des renseignements a été considérée comme une façon de protéger la vie privée des personnes. On a considéré que les renseignements anonymes ne posent pas d'enjeu de vie privée. Ces renseignements sont d'ailleurs exclus des actuels cadres de protection de la vie privée. Or, premièrement, les travaux d'Yves-Alexandre de Montjoye et al. ont montré qu'il est devenu de plus en plus difficile, voire impossible, d'anonymiser un ensemble de données (c'est-à-dire d'effacer les noms des personnes concernées et de faire en sorte que ces noms ne puissent être retrouvés par recoupement avec d'autres bases de données) puisque le croisement multiple des renseignements anonymes au moyen des outils d'analyse sophistiqués peut permettre de retracer l'identité des personnes. Deuxièmement, au-delà des risques de réidentification, l'analyse prédictive nous enseigne que des renseignements anonymes et anodins peuvent être combinés avec d'autres renseignements afin d'inférer des renseignements jugés privés et sensibles sur une personne et soulever des enjeux de vie privée. Alors que les cadres de protection attachent une importance à la nature des renseignements considérés au moment de la collecte, la nature des renseignements en tant que telle a de moins en moins d'importance. Au-delà du renseignement considéré en lui-même, *l'usage* du renseignement peut faire en sorte qu'il devient personnel ou non. De plus en plus d'experts insistent sur la nécessité de considérer le traitement des données dans son ensemble pour juger des enjeux de vie privée, et en particulier l'utilisation des renseignements au regard de leur impact sur les personnes et selon les contextes.

C’est notamment le cas de J.-M. Dinant et Y. Poullet qui affirment, au terme de leur rapport destiné au Comité des ministres du Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe :

> En conclusion, il est devenu de moins en moins pertinent de se poser la question de savoir si telle ou telle donnée est une donnée à caractère personnel, mais plutôt d’identifier les risques que fait courir l’utilisation des données issues des technologies de l’information et la communication dans un contexte particulier par un utilisateur donné et d’y apporter une réponse de principe.

Face aux défis que présente l’analyse prédictive des données massives, nous sommes d’avis que la protection de la vie privée doit focaliser davantage sur l’encadrement des utilisations des renseignements inférés au regard de leur impact sur les personnes plutôt que sur l’encadrement des pratiques de collecte des renseignements. Dit autrement, en plus d'inclure les mesures actuelles prévues pour limiter l'accès aux renseignements personnels, la protection de la vie privée devrait aussi inclure des limitations de certaines utilisations de renseignements sur les personnes, en particulier ceux qui ont été inférés à partir de données massives à distance et à l’insu de la personne concernée, en fonction des risques de préjudices que comporte l’utilisation de ces renseignements.

D’ailleurs, la réglementation en matière de protection des données met de plus en plus l'accent sur l'évaluation des risques, ainsi que le souligne A. Mantelero dans son rapport qui a mené aux *Lignes directrices sur l’intelligence artificielle et la protection des données* du Conseil de l’Europe adoptées en 2019. Mentionnons que le règlement de l’Union européenne sur l’IA adopté en avril 2021 adopte une approche fondée sur le risque (*risk-based approach*). L’idée de prédire les répercussions potentielles de l’intelligence artificielle sur le droit à la vie privée des personnes au regard des risques pour les personnes se retrouve dans la *Directive sur la prise de décision automatisée* adoptée par le gouvernement du Canada et qui est entrée en vigueur le 1er avril 2019.

Nous avons donc cherché à faire progresser la réflexion concernant l’encadrement des utilisations des renseignements inférés au regard de leurs risques de préjudices pour les personnes. Nous nous sommes d’abord attardés à ce que doit englober la notion de « risque ». Ensuite, nous nous sommes intéressés au cadre théorique qui permettrait de juger des traitements de renseignements inférés au regard de leurs risques de préjudices.

Jusqu’à maintenant, les risques associés à la vie privée étaient principalement compris au travers du prisme de l’identification. Or, à l’ère de l’analyse prédictive, la question même de l'identification comprise au sens strict (relier les renseignements de manière directe ou indirecte à l'identité civile de la personne, c’est-à-dire à son nom, prénom, adresse, numéro d’assurance sociale, etc.) devient secondaire. En effet, sur la base d’un profil établi, on peut caractériser une

personne naviguant sur Internet avec son ordinateur en fonction de critères jugés intimes et sensibles (par exemple des critères socio-économiques, psychologiques, philosophiques, de santé ou autres) et lui attribuer certaines décisions ou lui suggérer certaines actions sans même s'enquérir de son identité civile. En effet, le point de contact de la personne, soit l'appareil électronique utilisé, n'exige pas la connaissance de son identité au sens étroit du terme (Poullet, 2021, p. 49). L'enjeu ici est de *rapporter à une personne* des renseignements jugés intimes et sensibles et qui peuvent avoir un impact sur sa vie personnelle. En quelque sorte, on peut « individualiser » une personne et agir sur elle personne sans nécessairement « l'identifier » (Poullet, 2021, p. 49). C'est pourquoi nous sommes d'avis que le concept de « renseignement personnel » de la législation canadienne devrait inclure les risques d' « individualisation ». Il est intéressant de noter que le Conseil de l'Europe, dans ses *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, avance que les données à caractère personnel réfèrent à « toute information concernant une personne physique identifiée ou identifiable (la personne concernée) » et ajoute que « les données à caractère personnel englobent également toute information utilisée pour individualiser ou singulariser des personnes identifiées sur la base d'informations relatives au profilage d'un groupe » (p. 3).

Par ailleurs, les cadres actuels de protection de la vie privée se sont essentiellement attardés à protéger les libertés et les droits individuels. Or, les travaux des défenseurs d'une conception distinctive de la vie privée nommée « *group privacy* » nous ont appris que l'utilisation de technologies axées sur les données a des impacts non seulement sur les individus pris isolément, mais aussi pour les groupes d'individus en tant que groupes. Il s'agit de groupes de personnes qui partagent une identité générique générée au moyen d'algorithmes sur la base de l'analyse de données massives. Les renseignements obtenus à propos du groupe ne sont pas simplement applicables aux personnes qui composaient l'échantillon initial, mais généralisables et transposables à l'ensemble des personnes qui partagent les mêmes caractéristiques que celles de la population de base. Ainsi, ces renseignements émergents peuvent être applicables à des personnes dont les renseignements ne furent pas initialement partagés ou analysés. En plus de menacer les libertés de chaque individu pris séparément, l'analyse prédictive présente des risques de discrimination pour des groupes d'individus en tant que groupe sur la base d'attributs inférés par corrélations (par exemple, les personnes homosexuelles, les personnes de telle idéologie politique, les personnes avec telle habitude de vie, etc.). En ce sens, le traitement des données interpelle d'autres valeurs que celles liées aux libertés individuelles, notamment la valeur de justice sociale. Il nous semble pertinent d'élargir les préoccupations traditionnelles au-delà des préoccupations pour l'individu et de prendre en considération les risques pour les groupes d'individus, notamment au regard des risques de discrimination et de ciblage dont ils peuvent être affectés en tant que groupe. Bref, l'analyse des risques doit prendre en considération les groupes d'individus qui peuvent être affectés sur la base de traitement algorithmique de données massives.

La discrimination est bien évidemment un enjeu qui dépasse largement la protection de la vie privée. Toutefois, dans la mesure où il y a discrimination sur la base des renseignements inférés sur les individus, il peut être pertinent d'intervenir au moyen de mesures législatives sur la vie privée afin de contrer la discrimination. Pour reprendre l'expression de la professeure Austin, ces mesures fonctionneraient alors comme une protection anticipée (*anticipatory remedy*) pour un préjudice qui dépasse la vie privée en tant que telle. À l'instar de la *Loi sur la non-discrimination génétique* (L. C. 2017, ch. 3) adoptée par le Canada et qui interdit l'utilisation de renseignements génétiques pouvant mener à certaines formes de profilage et de discrimination, il pourrait être envisagé d'encadrer l'utilisation de certains renseignements inférés au regard des risques qu'ils soulèvent pour des individus ou des groupes d'individus. Il s'agirait en quelque sorte d'évaluer si la protection de la vie privée est la protection anticipée la plus efficace des mesures de protection et si le préjudice en question pourrait être empêché autrement et de coordonner les mesures de protection de la vie privée et d'autres mesures de protection. Ce qui peut être notamment le cas en ce qui concerne le ciblage psychologique (*psychological targeting*) qui consiste à extraire les profils psychologiques des personnes à partir de leurs empreintes numériques (par exemple, leurs *likes* Facebook, leurs *tweets* ou leurs enregistrements de cartes de crédit) afin d'influencer leurs attitudes, leurs émotions ou leurs comportements par le biais d'interventions psychologiques à grande échelle (Matz et al, 2020). L'efficacité du ciblage psychologique est directement liée au fait que le message soir adapté aux caractéristiques personnelles de la personne sur la base des inférences générées sur la personne. Encadrer certaines utilisations de ciblage psychologique au moyen des mesures sur la protection de la vie privée pourrait être examiné.

Nous sommes d'avis que la protection de la vie privée a aussi des impacts sur la vie démocratique dont il faut tenir compte. En effet, cette protection joue un rôle clé pour l'exercice de nombreux droits et libertés, notamment la liberté d'expression, la liberté d'association et de réunion. La protection de la vie privée est une condition importante pour la vie démocratique.

Le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dans ce passage des *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, nous invite à considérer les risques dans une large perspective : « L'utilisation des mégadonnées pouvant porter atteinte non seulement à la vie privée et à la protection des données de façon individuelle, mais également à la dimension collective de ces droits, les politiques préventives et l'évaluation des risques doivent tenir compte de l'impact juridique, social et éthique de cette utilisation, y compris au regard du droit à l'égalité de traitement et à la non-discrimination » (p. 4).

Bref, dans l'environnement numérique actuel et à l'ère de l'analyse prédictive, nous pensons qu'il est nécessaire d'élargir les préoccupations traditionnelles de nos cadres de protection de la vie privée afin d'éviter que la portée de ces cadres ne se limite qu'aux renseignements personnels compris dans un sens restrictif et que seuls les risques d'identification et d'atteinte aux libertés individuelles soient considérés. La protection de la vie privée ne réfère pas à la seule protection

d'individus considérés comme isolés et ne doit pas être pensée dans une perspective purement individualiste. Elle renvoie à la façon dont les personnes exercent leur autonomie privée et politique au sein d'une société. Ainsi que le formule Schwartz : « Rather than simply seeking to allow more and more individual control of personal data, we should view the normative function of information privacy as inhering in its relation to participatory democracy and individual self-determination… » (Poullet, 2019, p. 80). Dans son mémoire déposé dans le cadre des travaux de la *Déclaration de Montréal pour une intelligence artificielle responsable*, la Commission d'accès à l'information du Québec souligne à juste titre que « le droit à la vie privée est une valeur fondamentale essentielle à notre société démocratique et à l'autonomie de la personne qu'aucune technologie ne devrait remettre en question ». S'il est question de protéger adéquatement les personnes des risques soulevés par l'analyse prédictive et diminuer l'asymétrie de pouvoir qui existe entre les individus et les gouvernements et les entreprises qui utilisent les données, les efforts de réglementation ne doivent pas se limiter à l'autogestion de la vie privée par les individus, mais ils doivent s'appuyer sur une analyse des risques qui reconnaît l'importance de la vie privée dans toutes ses dimensions**.**

Il est alors nécessaire d'élaborer un cadre théorique qui permette de juger des utilisations de renseignements inférés au regard des risques de préjudices autant pour les individus que les groupes d'individus et qui reconnaît les avantages sociaux de la protection de la vie. Ce cadre doit éviter les limitations des cadres de protection actuels mentionnées au début de cette introduction. Nous avons expliqué dans notre rapport que la théorie de l'intégrité contextuelle d'Helen Nissenbaum constitue à cet égard un point de départ prometteur.

En effet, la théorie de l'intégrité contextuelle de Nissenbaum est présentée comme un cadre théorique servant à identifier les atteintes possibles au droit à la vie privée en vue de permettre la mise en place de protections légales adéquates. Cette théorie a été élaborée en considérant les enjeux soulevés par les technologies axées sur les données. C'est en constatant que le traitement de données peut soulever des enjeux de vie que Nissenbaum a élaboré sa théorie de l'intégrité contextuelle. Nissenbaum nous invite à penser la protection de la vie privée au-delà de la dichotomie du privé et du public qui a longtemps servi de référence pour penser la vie privée. Elle propose une façon de théoriser la fonction et la valeur de la vie privée à une époque où les données sont générées, diffusées et analysées à un rythme si rapide que le contrôle individuel sur les données semble ne semble pas toujours possible. Selon Nissenbaum, les enjeux de vie privée doivent être pensés dans une perspective plus large que l'approche individualiste. Sa théorie reconnaît l'impact de l'analyse prédictive sur les groupes d'individus, ainsi que le souligne C. Villani :

> Les travaux pionniers d'Helen Nissenbaum nous enseignent par exemple que les données sont des objets contextuels, qui peuvent renseigner simultanément sur plusieurs individus ou questions. Cela d'autant plus que, dans le cadre du *deep learning*, les données sont exploitées à grande échelle pour produire des corrélations qui peuvent concerner des groupes d'individus […] Un individu peut donc être protégé de manière

> granulaire contre la collecte d'une information qui l'identifie, mais cette protection ne couvre pas la configuration réticulaire (en réseau) que toute information revêt (p. 148).

La théorie de l'intégrité contextuelle insiste sur l'importance du contexte, importance qui est soulignée par plusieurs spécialistes et reconnue du point de vue juridique. Nissenbaum propose une conceptualisation du contexte en fonction de normes, et plus spécifiquement de « normes contextuelles d'information ». Les individus ne sont pas séparés les uns des autres, mais plutôt intégrés dans une collectivité. Ils interagissent les uns avec les autres à l'intérieur de contextes sociaux qui sont régis par des normes. Ces « normes contextuelles d'information » sont décrites au moyen de cinq paramètres clés : expéditeur, sujet, destinataire, attribut et principe de transmission. L'efficacité de cette conceptualisation du contexte pour mesurer ce que les gens jugent approprié ou inapproprié au regard du flux d'informations a été démontrée par plusieurs articles, dont cet article paru en 2022 : « Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates ».

Dans un séminaire en ligne de mars 2021, Nissenbaum explique que les récents développements numériques pourraient justifier le besoin d'ajouter un sixième paramètre, soit le « use parameter », qui préciserait les finalités de l'utilisation. Nous pensons qu'il est pertinent d'ajouter ce paramètre. La finalité de l'utilisation a d'ailleurs été prise en considération dans les récents articles qui ont appliqué le cadre d'analyse de Nissenbaum pour mesurer ce que les gens jugent approprié ou inapproprié au regard du flux d'informations dans des contextes variés. À cet égard, nous avons souligné que les considérations du critère de l'arrêt Oakes concernant les fins raisonnables demeurent pertinentes.

Nous avons expliqué dans notre rapport que la théorie contextuelle de Nissenbaum remplit sa visée descriptive, soit de fournir « a rigorous, substantive account of factors determining when people will perceive new information technologies and systems as threats to privacy » (p. 2). Toutefois, son cadre normatif n'est pas suffisant, tel que proposé, pour réaliser le deuxième aspect de l'objectif visé, soit de proposer «an approach to evaluating these systems and prescribing legitimate responses to them » (p. 2)). Nissenbaum soutient que ce qui importe, au-delà du fait qu'il y a ou non flux de renseignements personnels, c'est que le flux soit « approprié ». Sa position dépend ainsi lourdement des critères permettant son évaluation normative, c'est-à-dire des critères nous permettant d'évaluer si un flux particulier est « approprié ». Or, dans la dimension évaluative de l'heuristique décisionnelle de Nissenbaum, il est proposé de prendre en considération les facteurs moraux et politiques en fonction des valeurs, des fins et des objectifs spécifiques au contexte. Nous sommes d'avis que la protection des renseignements personnels doit s'enraciner dans la protection du droit à la vie privée et que cette protection doit se référer à des valeurs et principes moraux qui le sous-tendent. Les valeurs et les principes moraux doivent servir de standards éthiques pour l'évaluation des utilisations de données acceptables et inacceptables. Cependant, cette partie de l'heuristique ne contient pas suffisamment d'indications sur la manière de mener l'évaluation éthique et ne permet pas d'identifier

clairement les valeurs et les principes moraux qui doivent servir de standards éthiques pour l'évaluation des utilisations de données.

Dans la partie évaluative de l'heuristique décisionnelle de Nissenbaum, en particulier l'étape 7, il est demandé d'identifier les préjudices (*harms*) mis en cause avec l'utilisation des renseignements. Nous pensons que cette partie de l'heuristique qui porte sur les préjudices devrait être approfondie. Une meilleure analyse des préjudices faciliterait, nous semble-t-il, l'identification des valeurs et des principes moraux en jeu. Cette analyse bénéficierait des nombreux travaux menés ces dernières années par différents spécialistes au sujet des préjudices à la vie privée (*privacy harms*). À cet égard, D. Solove et D. Citron viennent de publier une typologie des préjudices à la vie privée qui se veut une mise à jour des quatre atteintes à la vie privée identifiées par William Prosser dans les années 60 et à la suite de travaux de spécialistes sur les préjudices. Cette typologie a l'avantage de prendre en considération l'impact de l'utilisation de renseignements sur les individus, les groupes d'individus et la société en général. Par exemple, l'un des préjudices identifiés par Solove et Citron est le « chilling effect ». Une utilisation de renseignements sous la forme d'une surveillance serait de nature à porter atteinte au principe d'autonomie et aux libertés individuelles, mais aussi d'avoir un effet négatif sur les interactions sociales de l'individu dans la mesure où une telle surveillance peut freiner la participation sociale.

L'amélioration des protections de la vie privée n'est pas un obstacle aux innombrables potentialités offertes par les technologies axées sur les données, mais plutôt la condition pour que ce potentiel soit exploité d'une manière responsable et socialement bénéfique. Il nous faut déterminer comment tirer avantage des données et assurer du même coup la protection du droit à la vie, qui est considérée une condition essentielle pour que les personnes puissent exercer leur autonomie au sein d'une société. Nous pensons qu'une approche centrée sur la prévention et la réduction des risques de préjudices découlant du traitement des renseignements personnels, tant pour les individus, les groupes d'individus et la société en général, est un élément nécessaire à une innovation responsable en ce qui concerne l'analyse prédictive. Pour les travaux de recherche à venir, il nous semble pertinent d'approfondir la compréhension des enjeux de protection de la vie privée par l'analyse contextuelle des risques de préjudices individuels et collectifs et qui intègrerait le cadre d'analyse de l'intégrité contextuelle proposé par Nissenbaum et l'identification des préjudices à la vie privée récemment proposée par des spécialistes, notamment la typologie qui vient d'être publiée par D. Solove et D. Citron. L'intégration de ces deux types de travaux n'a pas été effectuée jusqu'à maintenant. Une telle recherche, en plus d'éclairer les décideurs publics qui devront revoir le cadre législatif canadien de protection de la vie privée afin de mieux encadrer les utilisations de renseignements inférés, pourrait fournir des outils utiles pour la réalisation d'analyses d'impact relative à la protection des données. En outre, si le caractère sensible d'un renseignement s'évalue en fonction du contexte et des risques, comme l'explique P. Ohm dans son article « Sensitive information », cette recherche pourrait enrichir les réflexions sur la nature des renseignements sensibles et leur protection.

BIBLIOGRAPHIE

LIVRES, CHAPITRES DE LIVRES ET ARTICLES:

ABRAMS, Marin. (2014) « The Origins of Personal Data and its Implications for Governance », The Information Accountability Foundation

ACQUISTI, Alessandro, BRANDIMARTE, Laura et LOEWENSTEIN, George. (2015) « Privacy and human behavior in the age of information », *Science*, vol. 347, no. 1, p. 509-514.

ALLEN, Anita. (2013) « An Ethical Duty to Protect One's Own Information Privacy? », *Alabama Law Review*, vol. 64, no. 4, p. 845-866.

ALLEN, Anita L. (2011) *Unpopular privacy what must we hide?*, New-York, Oxford University Press, 259 p.

ANCIAUX, Arnaud et FARCHY Joëlle. (2015) « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue Internationale de Droit Économique*, vol. 29, no. 3, p. 307-331.

APTHORPE, Noah, VARGHESE, Sarah, & FEAMSTER, Nick. (2019) « Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA », *28th [USENIX] Security Symposium* ([USENIX] Security *19*), p. 123–140.

APTHORPE, Noah, SHVARTZSHNAIDER, Yan, MATHUR, Arunesh, REINSMAN, Dillon, & FEAMSTER, Nick (2018) « Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity », *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp),* Vol. 2, No. 2, p. 1-23.

ARENDT, Hannah. (1958) *The Human Condition*, Chicago : University of Chicago Press, 332 p.; *Condition de l'homme moderne*, Paris : Calmann-Lévy, 1994.

ARIES, Philippe et DUBY, Georges (éd.) (1985) *Histoire de la vie privée*, Paris : Éditions du Seuil, 5 tomes.

AUSTIN, John. (1955) *The province of jurisprudence determined and the uses of the study of jurisprudence*, Londres, Weidenfeld and Nicolson, 396 p.

AUSTIN, Lisa. (2003) « Privacy and the Question of Technology », *Law and Philosophy*, Vol. 22, p. 119-166.

BAROCAS, Solon et NISSENBAUM, Helen. (2014) « Big Data's End Run around Anonymity and Consent » dans *Privacy, Big Data and Public Good*, Cambridge University Press, 2014, p. 62.

BENN, Stanley I. (1971) « Privacy, freedom, and respect for persons » dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 223-244.

BENYEKHLEF, Karim et DÉZIEL, Pierre-Luc. (2018) *Le droit à la vie privée et droit québécois et canadien*, Éditions Yvon Blais, Montréal, 850 p.

BERNAL, Paul. (2014) *Internet Privacy Rights : Rights to Protect Autonomy*, Cambridge, Cambridge University Press.

BLACKBURN, Simon. (1996) « Analysis », dans *The Oxford Dictionary of Philosophy*, Oxford, Oxford University Press.

BLANKE, Jordan M. (2020) « Protection for "Inferences Drawn:" A Comparison between the General Data Protection Rule and the California Consumer Privacy Act », *SSRN Electronic Journal*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518164.

BLOUSTEIN, Edward J. (1964) « Privacy as an aspect of human dignity: An answer to Dean Prosser », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, p. 156-202.

BORGESIUS, Frederik J. Zuiderveen, (2016) « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation », *Computer Law & Security Review*, vol. 32, 2, p. 256-271.

BOURCIER, Danièle et FILIPPI, Primavera. (2018) « Vers un droit collectif sur les données de santé », *Revue de droit sanitaire et social*, Paris, Dalloz : https://hal.archives-ouvertes.fr/hal-01850925/document

BURDON, Mark. (2020), *Digital Data Collection and Information Privacy Law*, Cambridge University Press.

BUYERS, John et Susan BARTY (ed.), (2021) *Responsible AI. A Global Policy Framework*, McLean (Virg.), ITechLaw: https://inventory.algorithmwatch.org/

CALO, M. Ryan. (2011), « The Boundaries of Privacy Harm », *Indiana Law Journal*, vol. 86, p. 1131-1161.

CITRON, Danielle Keats., et SOLOVE, Daniel. (2018) « Risk and Anxiety : A Theory of Data Breach Harms », *96 Texas Law Review*, vol. 737, p. 738-786

CITRON, Danielle Keats et PASQUALE, Frank. (2014) « The Scored Society: Due Process for Automated Predictions », *Washington Law Review*, 89, 1, p. 1-34.

COFONE, N. Ignacio. (2019) « Antidiscriminatory Privacy », *SMU Law Review*, Vol. 72, p. 139-176.

COFONE, N. Ignacio et ROBERTSON, Z. Adriana. (2018) « Privacy Harms », *Hasting Law Journal*, Vol. 69, p. 1039-1098.

COHEN, Julie E. (2012) *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press.

COHEN, Julie E. (2000) « Examined lives: informational privacy and the subject as object », *Stanford Law Review*, vol. 52, no. 5, p. 1373–1438.

COHEN, Julie E. (1992), « Redescribing Privacy: Identity, Difference and the Abortion Controversy », *Columbia Journal of Gender and Law*, 3: 43–117.

COSTA, Luiz. (2016) *Virtuality and Capabilities in a World of Ambient Intelligence : New Challenges to Privacy and Data Protection*, Cham, Springer International Publishing (Law, Governance and Technology Series, vol. 32).

CRAWFORD, Kate et SCHULTZ, Jason. (2014) « Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms », *Boston College Law Review*, 55, 1, 4 : http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4

DECEW, Judith, (2018) « Privacy », *Stanford Encyclopedia of Philosophy*: https://plato.stanford.edu/entries/privacy/

DECEW, Judith, (1997) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press.

DÉZIEL, Pierre-Luc. (2019) « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », 465 *Développements récents en droit à la vie privée* 1, Éditions Yvon Blais / Barreau du Québec.

DÉZIEL, Pierre-Luc. (2018) « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », *Les cahiers de propriété intellectuelle*, vol. 30, no. 3, p. 827-847.

DUHIGG, Charles. (2012) « How Companies Learn Your Secrets », *New-York Times* (16 février 2012),
https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?p.

ELSHTAIN, Jean Bethke, (1995) *Democracy on Trial*, New York: Basic Books.

ETZIONI, Amitai, (1999) *The Limits of Privacy*, New York: Basic Books.

FLORIDI, Luciano et Josh COWLS. (2019) « A Unified Framework of Five Principles for AI in Society », *Harvard Data Science Review*, vol. 1,1
https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/7

FREY, R. (2000) « Privacy, Control, and Talk of Rights » *Social Philosophy and Policy*, vol. 17, no. 2, p. 45-67.

FRIED, Charles. (1968) « Privacy [a moral analysis] », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 203-222.

GAUTRAIS, Vincent et TRUDEL, Pierre. (2010) *Circulation des renseignements personnels et web 2.0.*, Montréal, Éditions Thémis, 231 p.

GAVISON, R. (1980) « Privacy and the limits of law », *The Yale Law Journal*, vol. 89, no. 3, p. 421–471.

GERDON, Frederic, NISSENBAUM, Helen, BACH, L. Ruben, KREUTER, Frauke, et ZINS Stefan. (2021). « Individual Acceptance of Using Health Data for Private and Public Benefit: Changes During the COVID-19 Pandemic », *Harvard Data Science Review, Special Issue 1* : *COVID-19: Unprecedented Challenges and Chances.*
GERSTEIN, Robert S. (1978) « Intimacy and Privacy », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 265-271.

GERSTEIN, Robert S. (1978) « Privacy and self-incrimination », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 245-264.

GUTWIRTH, Serge, LEENES, Ronald et DE HERT, Paul (éd.). (2014) *Reloading data protection : multidisciplinary insights and contemporary challenges*, Dordrecht, Springer, 369 p.

GUTWIRTH, Serge, POULLET, Yves, DE HERT, Paul, DE TERWANGNE, Cécile et NOUWT, Sjaak (éd.). (2009) *Reinventing Data Protection?*, Dordrecht, Springer.

HILDEBRANDT, Mireille. (2019) « Privacy as Protection of the Incomputable Self : From Agnostic to Agonistic Machine Learning », *Theoretical Inquiries in Law*, vol. 20, no. 1, p. 83-121.

HILDEBRANDT, Mireille. (2018) « Primitives of legal protection in the era of data-driven platforms »: https://ssrn.com/abstract=3140594

HIRSCH, Dennis. (2020) « From Individual Control to Social Protection: A New Paradigms for Privacy Law in the Age of Predictive Analytics », *Maryland Law Review*, Vol. 79, No. 2, p. 439-505.

HIRSCH, Dennis. (2017) « Predictive Analytics Law and Policy : A New Field Emerges », *I/S : A Journal of Law and Policy for the Information Society,* Vol. 14, p. 1-9.

HOPPE, Sabrina, LOETSCHER, Tobias. MOREY, Stephanie A et BULLING, Andreas (2018). « Eye Movements During Everyday Behavior Predict Personality Traits », *Frontiers in Human Neuroscience* 12.

INNESS, C. Julie., (1996) *Privacy, Intimacy, and Isolation*, Oxford, Oxford University Press, 176 p.

JERNIGAN, Carter et MISTREE, Behram, F. T., (2009) « Gaydar: Facebook Friendships Expose Sexual Orientation », *First Monday* 14, no. 10, 25.

JOBIN, Anna *et al.* (2019) « Artificial Intelligence: the global landscape of ethics guidelines », *Health Ethics and Policy Lab, ETH*, p. 1 - 42.

KAMMOURIEH, L. et al., (2017) « Group privacy in the age of big data » dans Taylor, L., Floridi, L. et van der Sloot, B. éd., *Group Privacy: new challenges of data technologies*. Dordrecht: Springer, 2017, p. 65.

KATIKALAPUDI, R. et al., (2012) « Associating Internet Usage with Depressive Behavior among College Students », *IEEE Technology and Society Magazine,* 31, no. 4.

KEULEN, Sjoerd et KROEZE, Ronald, (2018) « Privacy from a Historical Perspective », *The Handbook of Privacy Studies*, Amsterdam University Press: https://doi.org/10.1515/9789048540136-002

KOSINSKI, Michal. (2021) « Facial recognition technology can expose political orientation from naturalistic facial images », *Scientific Reports*, 11, 100 : https://doi.org/10.1038/s41598-020-79310-1

KOSINSKI, Michal et WANG, Yilun. (2018) « Deep neural networks are more accurate than humans at detecting sexual orientation from facial image », *Journal of Personality and Social Psychology*, vol. 114, no. 2, p. 246-257.

KOSINSKI, Michal, STILLWELL, David et GRAEPEL, Thore. (2013) « Private traits and attributes are predictable from digital records of human behavior », *Proceedings of the National Academy of Sciences*, vol. 110, no. 15, p. 5802-5805.

KROTOSZYNSKI, Ronald J. (2016) *Privacy Revisited : A Global Perspective On the Right to Be Left Alone*, New-York, Oxford University Press, 312 p.

LANE, Julia, STODDEN, Victoria, BENDER, Stefan et NISSENBAUM, Helen (éd.). (2014) *Privacy, Big Data and the Public Good : Framework for Engagement*, Cambridge, Cambridge University Press, 342 p.

LEVER, Annabelle (2013) *A Democratic Conception of Privacy*, Londres, AuthorHouse, 174 p.

LEVER, Annabelle. (2012) *On Privacy*, New-York, Routledge, 100 p.

MACLURE, Jocelyn et SAINT-PIERRE, Marie-Noëlle. (2018) « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », Les cahiers de propriété intellectuelle, vol. 30, n. 3, p. 741-765.
https://www.ethique.gouv.qc.ca/assets/documents/CPI_Maclure_Saint-Pierre.pdf

MACKINNON, Catherine, (1989) *Toward a Feminist Theory of the State*, Cambridge, MA: Harvard University Press.

MAI, Jens-Erik, (2016) « Big data privacy: The datafication of personal information », *The Information Society*, vol. 32, no. 3, p. 192-199.

MAI, Jens-Erik, (2016) « Three Models of Privacy: New Perspectives on Informational Privacy », *Nordicom Review*, 37, p. 171-175.

MANTELERO, Alessandro. (2016) « Personal data for decisional purposes in the age of analytics : From an individual to a collective dimension of data protection », *Computer Law and Security Review*, vol. 32, no. 2, p. 238-255.

MARTIN, Kirsten, et NISSENBAUM, Helen, (2017) « Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables », *Columbia Science and Technology Law Review* Vol. 18, p. 176-218.

MATZ, Sandra C., KOSINSKI, Michal, NAVE, Gideon et STILLWELL, David J. (2017) « Psychological targeting as an effective approach to digital mass persuasion », *Proceedings of the National Academy of Sciences of the United States of America*, vol. 114, no. 48, p. 12714-12719.

MAVRIKI, Paola et KARYDA, Maria. (2020) « Automated data-driven profiling : threats for group privacy », *Information and Computer Security*, vol. 28, no. 2, p. 183-197.

MAYEDA, Graham. (2015) « My neighbour's kid just bought a drone... : new paradigms for privacy law in Canada », *National Journal of Constitutional Law*, vol. 35, no. 1, p. 59-84.

MILLS, Jon L. (2008) *Privacy : The Lost Right*, New-York, Oxford University Press, 391 p.

MISLOVE, A. et al., (2010) « You Are Who You Know: Inferring User Profiles in Online Social Networks », *WSDM '10 Proceedings of the Third ACM International Conference on Web Search and Data Mining*, New York, NY:ACM Press.

MONTGOMERY, F. H. et al., (2013) « Monitoring Student Internet Patterns: Big Brother or Promoting Mental Health? », *Journal of Technology in Human Services*, 31, no. 1.

MONTJOYE, Yves-Alexandre, RADAELLI, Laura., SINGH, Vivek Kumar, PENTLAND, Alex Sandy, (2015) « Unique in the shopping mall: On the reidentifiability of credit card metadata », *Science,* 357: 6221, 536-539: https://science.sciencemag.org/content/347/6221/536

MOOR, James H. (1997) « Towards a theory of privacy in the information age » *ACM SIGCAS Computers and Society*, vol. 27, no. 3, p. 27–32.

MOORE, Adam D. (2010) *Privacy Rights. Moral and Legal Foundations*, Penn State University Press, 2010, 248 p.

NISSENBAUM, Helen, (2019) « Contextual Integrity Up and Down the Data Food Chain », *Theoretical Inquiries in Law,* Vol. 20, No. 1, p. 221-256.

NISSENBAUM, Helen., (2015) « Respect for Context as a Benchmark for Privacy Online: What it is and isn't », dans ROESSLER, Burt, et MOKROSINSKA, David., (éd.), *Social Dimensions of Privacy*, Cambridge, Cambridge University Press. Réimprimé dans MOORE, Adam., (éd.), *Privacy, Security and Accountability : Ethics, Law, and Policy*, Londres, New York, Rowman & Littlefield International, 2016, 39-62.

NISSENBAUM, Helen., (2011) « A Contextual Approach to Privacy Online », *Daedalus* Vol. 140, No. 4, Printemps 2011, p. 32-48.

NISSENBAUM, Helen. (2010) *Privacy in Context*, Stanford, Stanford University Press, 288 p.

OHM, Paul. (2015) « Sensitive Information », Southern California Law review, vol. 88 ; 5, p. 1125-1196.

OHM, Paul. (2014) « Changing the Rules : General Principles for Data Use and Analysis », dans J. LANE, V. STODDEN, S. BENDER et H. NISSENBAUM (éd.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Cambridge, Cambridge University Press , p. 96-111.

OHM, Paul. (2010) « Broken promises of privacy: responding to the surprising failure of anonymization », UCLA LAW REVIEW, 57, p. 1701-1777.

O'NEIL, Cathy. (2016) *Weapons of Math Destruction*, New York, Broadway Books, 275 p.

OOSTVEEN, Manon., (2016) « Identifiability and the applicability of data protection to big data », *International Data Law*, vol. 6, no. 4, p. 309

PARENT, W. A. (1983) « Privacy, Morality and the Law », *Philosophy and Public Affairs*, vol. 12, no. 4, p. 269-288.

PATEMAN, Carole (1989), « Feminist Critiques of the Public/Private Dichotomy » dans *The Disorder of Women: Democracy, Feminism, and Political Theory*, Stanford: Stanford University Press.

PEIKOFF, L. Amy., (2008) « Beyond Reductionism : Reconsidering the Right to Privacy, *NYU Journal of Law and Liberty*, Vol. 3, No. 1, p. 3-41.

PKIFT, Paula, et NISSEMBAUM, Helen., (2017) « Metadata in Context – An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program », *I/S: A Journal of Law and Policy for the Information Society,* Vol. 13, No. 2, p. 332-372.

POULLET, Yves., (2019), *La vie privée à l'heure de la société du numérique*, Belgique : Larcier.

POULLET, Yves., (2020), *Le RGPD face aux défis de l'intelligence artificielle*, Belgique : Larcier.

POSNER, Richard. (1978) « The Right of Privacy », *Georgia Law Review*, vol. 12, no. 3, p. 393-422.

PROSSER, William L. (1984) « Privacy [a legal analysis] », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, p. 104-155.

POST, Robert C., (2001) « Three Concepts of Privacy », 89 GEO. L.J. 2087.

PURTOVA, Nadezhda. (2018) « The law of everything. Broad concept of personal data and the future of EU data protection law », *Law, Innovation and Technology*, vol. 10, no. 1, p. 40-81.

RACHELS, James. (1975). « Why privacy is important », *Philosophy & Public Affairs*, vol. 4, no. 4 (juillet 1975), p. 323–333.

REGAN, Priscilla M. (2002) « Privacy as a common good in the digital world », *Information, Communication & Society*, vol. 5, no. 3, p. 382–405.

REIMAN, Jeffrey H. (1976) « Privacy, intimacy, and personhood » dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 300-316

ROCHER, Luc, HENDRICKX, Julien M. et MONTJOYE (de), Yves Alexandre. (2019) « Estimating the success of re-identifications in incomplete datasets using generative models », *Nature Communications*, vol. 10, no. 1, p. 3069–3069.

ROESSLER, Beate et MOKROSINSKA, Dorota (éd.). (2015) *Social Dimension of Privacy : Interdisciplinary Perspectives*, Cambridge, Cambridge University Press, 360 p.

ROUVROY, Antoinette et STIEGLER, Bernard. (2016) « The digital regime of truth: from the algorithmic governmentality to a new rule of law », *La Deleuziana*, 3: http://www.crid.be/pdf/public/8004.pdf

ROUVROY, Antoinette et BERNS, Thomas. (2013) « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation? », *Réseaux*, 1, no. 177, p. 163-196.

ROUVROY, Antoinette. (2008) « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, vol. 2, no. 1, art. 3 : https://ssrn.com/abstract=1013984

RULE, B. James. (2019) « Contextual Integrity and its Discontents: A Critique of Helen Nissenbaum's Normative Arguments », *Policy and Internet*, Vol. 11, No. 3, p. 260-279.

RYAN, Mark et Bernd CARSTEN STAHL. (2021) « Artificial Intelligence Ethics Guideline for Developers and Users: clarifying their content and normative implications », *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 1, pp. 61 – 86.

SAX, Marijn, (2018). « Privacy from an Ethical Perspective », dans B. VAN DER SLOT et DE GROOT, A. (éd.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* , Amsterdam: Amsterdam University Press.

SCANLON, Thomas., (1975) « Thomson on Privacy », *Philosophy and Public Affairs*, Vol. 4, No. 4, p. 315-322.

SCASSA, Teresa. (2020) « A Human Right-Based Approach to Data Protection in Canada », dans E. DUBOIS et F. MARTIN-BARITEAU (éd.), *Citizenship in a Connected Canada: A Research and Policy Agenda*, Ottawa, University of Ottawa Press: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620450

SCHOEMAN, Ferdinand David. (1992) *Privacy and Social Freedom*, Cambridge, Cambridge University Press, 225 p.

SCHOEMAN, F. (1984) « Privacy: Philosophical dimensions of the literature », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 1-33.

SCHOEMAN, F. (1984) « Privacy and intimate information », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 403-418.

SHVARTZSHNAIDER, Yan *et al.* (2016) « Learning privacy expectations by crowdsourcing contextual informational norms », *Fourth AAAI Conference on Human Computation and Crowdsourcing.*

SOLOVE, J. Daniel, et KEATS CITRON, Danielle., (2021) « Privacy Harms », *GW Law Faculty Publications and Other Works*, Vol. 1534. http://dx.doi.org/10.2139/ssrn.3782222.

SOLOVE, Daniel. (2013) « Introduction: privacy self-management and the consent dilemma », *Harvard Law Review*, vol. 126, no. 7, p. 1880–1903.

SOLOVE, Daniel. (2008) *Understanding Privacy*, Cambridge, London, Harvard University Press, 257 p.

SOLOVE, Daniel. (2006) « A Taxonomy of Privacy », *University of Pennsylvania Law Review*, vol. 154, no. 3, p. 477-560.

SOLOVE, Daniel. (2002) « Conceptualizing Privacy », *California law Review*, vol. 90, p. 1087-1154

TAVANI, Herman T. (2008) « Informational Privacy : Concepts, Theories, and Controversies » dans *The Handbook of Information and Computer Ethics*, New Jersey, John Wiley & Sons.

TAVANI, Herman T. (2007) « Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy », *Metaphilosophy*, vol. 38, no. 1, p. 1-22.

TAYLOR, Linnet, FLORIDI, Luciano et VAN DER SLOOT, Bart (éd.) (2017) *Group Privacy: new challenges of data technologies*, Dordrecht: Springer, 237 p.

TENE, Omer et POLONETSKY, Jules. (2013) « Big Data for All: Privacy and User Control in the Age of Analytics », *Northwestern Journal of Technology and Intellectual Property*, 239.

THOMSON, Judith J. (1975) « The Right to privacy », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 272-289.

TIEDEMANN, Paul. (2020) *Philosophical Foundation of Human Right*, Springer, 406 p.

UTZ, Christine, *et al.* (2021) « Apps against the spread : Privacy implications and user acceptance of COVID-19-related smartphone apps on three continents », *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. May 2021.

VÉLIZ, Carissa. (2020) *Privacy Is Power: Why and How You Should Take Back Control of Your Data,* Londres, Bantam Press, 268 p.

WACHTER, Sandra et MITTELSTADT, Brent. (2018) « A Right to Reasonable Inferences : Re-Thinking Data Protection Law in the Age of Big Data and AI », *Columbia Business Law Review*, vol. 2019, no. 2,:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

WARREN, Samuel D. et BRANDEIS, Louis D. (1890) « The right to privacy [the implicit made explicit] », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 75-103.

WASSERSTROM, Richard A. (1978) « Privacy: some arguments and assumptions », dans Richard BRONAUGH (éd.), *Philosophical Law. Authority, Equality, Adjucation, Privacy*, Westport, Greenwood Press.

WESTIN, Alan. (1967) *Privacy and Freedom*, New-York, Ig Publishing, 558 p.

WESTIN, Alan. (1967) « The origins of modern claims to privacy », dans F. SCHOEMAN (éd.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press, 1984, p. 56-74.

WOODROW, Hartzog., (2021) « What Is Privacy? That's the Wrong Question », *University of Chicago Law Review*, Vol. 88, No. 7, p. 1677-1688.

YOUYOU, Wu, STILLWELL, David, SCHWARTZ, H. Andrew et KONSINSKI, Michal. (2017) « Birds of a Feather Do Flock Together : Behavior-Based Personality-Assessment Method

Reveals Personality Similarity Among Couples and Friends », *Psychological Science*, vol. 28, no. 3, p. 276-284.

ZHANG, Shikun, *et al.* (2021) « "Did you know this camera tracks your mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics » *Proceedings on Privacy Enhancing Technologies*, vol. 2, p. 282–304.

ZHANG, Shikun, *et al.* (2022) « Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates », *in* 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT'22), June 21–24, 2022, Seoul, Republic of Korea. ACM, New York, NY, USA: https://doi.org/10.1145/3531146.3533222

RAPPORTS, MÉMOIRES ET DOCUMENTS DE CONSULTATIONS :

BORGESIUS, Frederik J. Zuiderveen, (2018) « Discrimination, intelligence artificielle et décisions algorithmiques », Strasbourg, Direction générale de la Démocratie, Conseil de l'Europe : https://rm.coe.int/etude-sur-discrimination-intelligence-artificielle-et-decisions-algori/1680925d84

CHRISTL, Wolfie. (2017) *Corporate Surveillance in Everyday Life: How Company Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*, Vienne, Craked Labs, 93 p.

CHRISTL, Wolfie. (2017) *Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. How Companies Use Personal Data Against People*, Craked Labs, 56 p.

CHRISTL, Wolfie et SPIEKERMANN, Sarah. (2016) *Networks of Control : A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*, Vienne, Facultas, 165 p.

COFONE, Ignacio. (2020) « Propositions stratégiques aux fins de la réforme de la LPRPDE élaborées en réponse au rapport sur l'intelligence artificielle » : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pol-ai_202011/

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2020) « Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE » : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2019) *Rapport annuel au Parlement 2018-2019 concernant la Loi sur la protection des renseignements personnels*, Canada, 23 p. : https://www.priv.gc.ca/media/4995/ar_2018-2019_pa_fra.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2018) *Document d'orientation sur les pratiques inacceptables du traitement des données : Interprétation et application du paragraphe 5(3)* : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gd_53_201805/

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2014) « Métadonnées et vie privée. Un aperçu technique et juridique » : https://www.priv.gc.ca/media/1793/md_201410_f.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2012) « L'ère de l'analyse prédictive : des tendances aux prédictions » : https://www.priv.gc.ca/media/1755/pa_201208_f.pdf

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC. (2018) *Pour un développement responsable de l'intelligence artificielle qui respecte le droit à la vie privée et responsabilise tous les acteurs impliqués*, Québec, 6 p. : https://www.cai.gouv.qc.ca/documents/CAI_M_IA.pdf

COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE. (2019) *Réponse au document de consultation sur l'intelligence artificielle de la commission d'accès à l'information du Québec*, Québec, 21 p. : https://www.ethique.gouv.qc.ca/media/1338/cest_ia_cai_2020.pdf

COMMISSION DE RÉFLEXION SUR L'ÉTHIQUE DE LA RECHERCHE ET SCIENCE ET TECHNOLOGIES DU NUMÉRIQUE D'ALLISTENE (CERNA). (2017) *Éthique de la recherche en apprentissage machine*, France, Allistene,, 49 p. http://cerna-ethics-allistene.org/digitalAssets/53/53991_cerna___thique_apprentissage.pdf

COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ. (2019) *Données massives et santé : une nouvelle approche des enjeux éthique (avis 130)*, France, 92 p. : https://www.ccne-ethique.fr/sites/default/files/avis_130.pdf

DÉZIEL, Pierre-Luc, BENYEKHLEF, Karim et GAUMONT, Eve. (2020) *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA*, Observatoire International sur les Impacts Sociétaux de l'IA et du Numérique, Québec, 38 p.

CONSEIL DE L'EUROPE. (2017) *Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées*, p.1 : https://rm.coe.int/lignes-directrices-sur-la-protection-des-personnes-a-l-egard-du-traite/16806f06d1

CONSEIL DE L'EUROPE. (2018) *Lignes directrices sur l'intelligence artificielle et la protection des données*.

EUROPEAN COMMISSION (ARTICLE 29 DATA PROTECTION WORKING PARTY). (2013) *Opinion 03/2013 on purpose limitation*.

GROUPE DES POLITIQUES ET DE LA RECHERCHE DU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. (2016) *Consentement et protection de la vie privée : Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques*, Canada, 36 p.:

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/2016/consent_201605/

MANTELERO, Alessandro. (2019). *Rapport sur l'intelligence artificielle. Intelligence artificielle et protection des données : enjeux et solutions possibles*.

NATIONS UNIES (CONSEIL DES DROITS DE L'HOMME). (2017) Résolution 37/7 du Conseil des droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, A/HRC/RES/37/4.

PRIVACY INTERNATIONAL. (2017) *Examples of Data Points Used in Profiling* : https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf

VILLANI, Cédric et al. (2018) *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, France, 233 p. : https://www.c2rp.fr/sites/default/files/atoms/files/c2rp-rapport-villani-donner-un-sens-a-intelligence-artificielle.pdf