Université du Québec
à Rimouski

L'évaluation des risques et des préjudices portés à la vie privée en contexte de transformation numérique

Considérations éthiques autour de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25)

Mémoire présenté

dans le cadre du programme de maîtrise en éthique

en vue de l'obtention du grade de maître ès arts

PAR

© CARBONNEAU MARTIN

Octobre 2022

Composition du jury :

Hazar Haidar, présidente du jury, Université du Québec à Rimouski

Dany Rondeau, directrice de recherche, Université du Québec à Rimouski

Daniel J. Caron, examinateur externe, École nationale d'administration publique

Dépôt initial le 4 août 2022 Dépôt final le 19 octobre 2022

REMERCIEMENTS

Je tiens d'abord à remercier Dany, ma directrice de recherche pour ses précieux commentaires et ses suggestions, mais également pour sa patience et sa compréhension face à mes nombreuses volte-face tout au long du travail derrière ce mémoire. Ses bons mots et ses conseils vont continuer à m'accompagner professionnellement.

Je souligne l'apport de mes anciens collègues de travail Diane, Xavier, Caroline, Stéphanie-Pascale et Ingrid. Mes échanges passés avec eux ont irrigué certaines des réflexions présentées dans ce mémoire.

Une mention spéciale à mon bon ami Pierre-Olivier. Chaque fois que j'avais idée de tout lâcher, je me rappelais la journée fatidique où il m'a candidement dit « toi, tu ne termines jamais rien » (ce qui est faux dans l'absolu). L'orgueil aidant, cet événement a depuis été un important catalyseur de motivation. Merci POC! Maintenant, dans un échange de bons procédés, j'attends de pied ferme sa réfutation du principe de non-contradiction.

Merci aussi à M. Perron qui m'a fait réaliser qu'il ne faut pas attendre d'en arriver *in extremis* pour tenter de réaliser un objectif personnel.

Je ne pourrais passer sous silence le support inconditionnel de mes parents Marie-Andrée et Julien-Marie. Je les remercie de m'avoir laissé faire à ma tête tout au long de mon cheminement scolaire : ce fut long, mais c'est désormais payant!

Et finalement, mille milliards de mercis à Pascale et Édouard. Ces deux personnes, si chères à mes yeux, m'ont attendu, m'ont supporté et m'ont enduré dans cette aventure. Je nous ai volé plusieurs moments tout au long des dernières années. J'entends bien me reprendre.

RÉSUMÉ

Dès septembre 2023, les organismes publics québécois et les entreprises du secteur privé faisant affaire au Québec devront produire obligatoirement une évaluation des facteurs relatifs à la vie privée pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels. L'objectif de ce mémoire est d'explorer l'une des composantes de ce type d'évaluation, soit l'évaluation des risques et des préjudices portés à la vie privée des personnes concernées par les projets assujettis à cette obligation.

À partir d'une recherche théorique et conceptuelle, il s'agira de définir quelle est la nature des risques et des préjudices dont devront tenir compte ces organisations dans leur processus d'évaluation. En prenant pour point de départ que les objectifs de tels processus d'évaluation sont de responsabiliser les organisations qui collectent, utilisent et communiquent des renseignements personnels et de hausser le niveau de protection de la vie privée auquel les citoyennes et citoyens et les consommatrices et consommateurs peuvent s'attendre, il paraît nécessaire d'avoir une certaine compréhension commune de ce que sont les risques et les préjudices portés à la vie privée et de ce que veut dire l'expression « protéger la vie privée » pour atteindre véritablement ces objectifs. L'hypothèse à l'étude dans ce mémoire est que les risques et les préjudices portés à la vie privée s'apparentent en fait aux risques éthiques. Ainsi, l'évaluation des facteurs relatifs à la vie privée devrait, du moins dans sa composante « gestion des risques », s'apparenter à une évaluation éthique, et ce, au moins pour certaines catégories de projets.

Certains enjeux éthiques liés plus spécifiquement à la réalisation des évaluations des facteurs relatifs à la vie privée sont également abordés succinctement dans ce mémoire. Il s'agira d'abord d'envisager l'impact qu'auront les caractéristiques des risques et des préjudices portés à la vie privée sur la capacité qu'aura leur évaluation à rivaliser avec les différents impératifs qui sous-tendent la transformation numérique des organisations, puis d'aborder la question de la posture professionnelle des personnes qui seront appelées à réaliser cette évaluation.

Mots clés : vie privée, protection de la vie privée, protection des renseignements personnels, risques, préjudices, gestion des risques, évaluation des facteurs relatifs à la vie privée, projets informatiques, posture professionnelle

ABSTRACT

As of September 2023, Quebec public bodies and private sector companies doing business in Quebec will be required to produce a privacy impact assessment for any project involving the acquisition, development or redesign of an information system or electronic service delivery that involves personal information. The purpose of this thesis is to explore one of the components of such an assessment, which is the assessment of risks and harms to the privacy of individuals involved in projects subject to this obligation.

Based on theoretical and conceptual research, we will define the nature of the risks and harms that these organizations must consider in their evaluation process. Taking as a starting point that the goals of such assessment processes are to hold accountable organizations that collect, use and disclose personal information and to raise the level of privacy protection that citizens and consumers can expect, it seems necessary to have some common understanding of what privacy risks and harms are and what the term "privacy protection" means in order to truly achieve these goals. The hypothesis under consideration in this paper is that privacy risks and harms are in fact similar to ethical risks. Thus, privacy impact assessment should, when it comes to its risk management component, be akin to an ethic assessment, at least for certain categories of projects.

Some of the ethical issues related to the conduct of privacy impact assessments are also briefly discussed. After considering the impact that the characteristics of privacy risks and harms will have on the ability of the assessment to compete with the various imperatives that underlie the digital transformation of organizations, we will address the question of the professional posture of those persons who will be called upon to carry out this assessment.

Keywords: privacy, privacy protection, privacy, risk, harms, risk management, privacy impact assessment, IT project, professional posture

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

AIPD Analyse d'impact à la protection des données

CAI Commission d'accès à l'information du Québec

CDPDJ Commission des droits de la personne et de la protection de la jeunesse

CEST Commission de l'éthique en science et en technologie

COMEST Commission mondiale d'éthique des connaissances scientifiques et des technologies

CPVPC Commissariat à la protection de la vie privée du Canada

ÉFVP Évaluation des facteurs relatifs à la vie privée

ISO Organisation internationale de normalisation

Loi sur l'accès *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (loi provinciale québécoise)*

LPRP *Loi sur la protection des renseignements personnels* (loi fédérale canadienne)

Loi sur le privé *Loi sur la protection des renseignements personnels dans le secteur privé (loi provinciale québécoise)*

OCDE *Organisation de coopération et de développement économiques*

PIA *Privacy impact assessment*

RGPD *Règlement général sur la protection des données*

SRIDAIL	Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité

INTRODUCTION GÉNÉRALE

Privacy is dead—get over it!
– Scott McNealy, ex-PDG de Sun Microsystems

Privacy is too important to let it wither. Who you are and what you do is nobody's business. You are not a product to be turned into data and fed to predators for a price. You are not for sale. You are a citizen, and you are *owned* privacy.
– Carissa Véliz, *Privacy is Power*

Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.
– Judith Jarvis Thomson, *The Right to Privacy*

Les outils numériques font désormais partie de l'ossature de nos sociétés occidentales. Mais bien que le recours aux technologies de l'information s'imposait déjà bien avant la crise sanitaire engendrée par la pandémie de SARS-COV-2, cette dernière aura servi de catalyseur à la transformation numérique en renforçant la position des outils technologiques à titre de passerelles essentielles de socialisation et de communication. Ces derniers auront été autant d'outils nous permettant de maintenir le contact avec nos proches, de continuer à consommer malgré les confinements répétés et de continuer à vaquer à nos occupations à distance. Les organisations, comme les personnes, en ont grandement besoin. Comme le souligne la philosophe Carissa Véliz :

> As a result of the pandemic, however, any lingering illusion of voluntariness in the use of technology has disappeared. It is not only citizens who rely on big tech to perform their jobs: businesses, universities, health services, and governments need the platforms to carry out their everyday functions. All over the world, governmental and diplomatic meetings are being carried out on platforms such as Zoom and Teams. (2021, p. 10)

L'organisation de la société s'articule désormais en grande partie autour du numérique et la liberté qu'ont les individus à y avoir recours s'amenuise au fur et à mesure que les technologies s'instillent dans le quotidien. Cette tendance hégémonique du numérique s'observe facilement au Québec, comme le démontrent les nombreuses enquêtes produites par l'Académie de transformation numérique de l'Université Laval. Ces enquêtes montrent que le recours accru aux technologies numériques touche la plupart des secteurs. C'est le cas de la consommation des services publics (ATN, 2022c), des services bancaires (ATN, 2021c) et de l'achat en ligne (ATN, 2022b; Statistique Canada, 2021). Les objets connectés se multiplient dans les maisons (ATN, 2021b), le temps passé en ligne par les enfants d'âge scolaire ou par les aînés augmente (ATN, 2021d, 2022a) et l'usage du numérique dans les écoles se généralise (ATN, 2021a). L'industrie culturelle connaît elle aussi son lot de mutations. La migration des médias et des produits culturels vers les plateformes numériques et la raréfaction de l'offre des médias traditionnels changent certains comportements des consommateurs. Ces derniers se tournent désormais vers cette nouvelle offre culturelle pour se divertir ou pour s'informer (CEFRIO, 2019; Commission de la culture et de l'éducation, 2020; Gouvernement du Canada, 2020; ISQ, 2021b). Les entreprises aussi ont recours à Internet et aux technologies numériques dans une très grande proportion (ISQ, 2022).

La professeure de science des communications Helen Nissenbaum nous rappelle que l'usage généralisé d'une technologie ne s'impose pas seule : il s'accompagne de la mise en place de tout un arsenal d'infrastructures physiques, de politiques publiques et de normes sociales, culturelles et juridiques. L'adhésion massive et collective à une technologie réorganise la société et modifie les mœurs, les comportements et les habitudes de ses membres. Nissenbaum prend l'exemple du téléphone pour illustrer son point :

> To begin, consider the familiar telephone sitting on your desk. Upon the initial reckoning you could see it as a self-standing technical device (think of the phone in the box when you purchased it), but its capacity to function as a telephone, enabling communication at a distance, requires that it be connected to a complex telecommunications system including all the necessary hardware and software. Beyond these, a proper functioning telecommunications system depends on a host of social, political, and economic arrangements. (2009, p. 4-5)

Le déploiement du téléphone s'est accompagné de la mise en place d'un réseau filaire, de dispositifs de commutation des appels et a mené à l'adoption de normes technologiques et juridiques. L'interdiction d'écouter et d'enregistrer les discussions à l'insu des interlocuteurs représente un bel exemple d'une norme juridique associée à la protection de la vie privée. L'arrivée du téléphone dans les demeures et dans les milieux de travail a également modifié les habitudes des gens en leur offrant de nouvelles possibilités d'organisation de leur quotidien. Ainsi, comme le poursuit Nissenbaum :

> When observing, say its effects on the workplace hierarchy, on the home, on the friendship, on the aged, on law enforcement, on urban development, and so forth, we do not mean the telephone in the box but the telephone connected to a telecommunication system, regulated by a host of technical standards, public policies, and even social and cultural norms. […] I am thinking of them as socio-technical; they affect us not purely by dint of physical or material properties but by properties they acquire as systems and webs of meaning. (2009, p. 5)

À l'instar du téléphone, l'implantation des technologies numériques (pensons entre autres aux algorithmes d'intelligence artificielle, aux outils exploitant les chaînes de blocs, aux cryptomonnaies, à la biométrie, aux objets connectés et à l'identité numérique) dans la plupart des sphères de l'activité humaine (en éducation, en santé, pour le commerce, les finances, le divertissement, pour les relations entre le citoyen et l'État, etc.) transforme tout autant l'organisation sociale. Cette transition vers le numérique s'accompagne d'un réalignement des sociétés similaire à ceux que les sociétés ont subi à la suite de l'invention de la machine à vapeur, à l'électrification des villes ou à l'urbanisme axé autour du tout à l'automobile. Ainsi, tout système technologique n'est pas seulement technologique, il est, pour reprendre le terme de Nissenbaum, sociotechnique.

Pour le citoyen moyen, il existe une pression certaine à se conformer aux pratiques découlant de l'utilisation du numérique. Le philosophe Mark Hunyadi utilise le terme de « mode de vie » pour désigner cet « ensemble des pratiques concrètes qui façonnent effectivement les comportements de chacun en produisant des attentes auxquelles, pour se socialiser, les individus se conforment » (2015, p. 44). Le mode de vie consiste en un sous-produit de ces systèmes sociotechniques dont Nissenbaum fait mention. Lorsqu'une

nouveauté technologique se met en place et que son usage se généralise, elle instille des attentes comportementales qui s'imposent subrepticement aux individus. Ces derniers sont alors confrontés au fait de choisir l'intégration de cette technologie dans leur quotidien ou de vivre une certaine forme de marginalité, sans pouvoir profiter des bénéfices de ces technologies. La possibilité de choisir un style de vie qui s'écarte radicalement des principales attentes comportementales induites par un mode de vie se fait alors que les solutions de remplacement se raréfient et que l'effort pour pallier cette rareté s'accentue. L'action dans cette marge se fait au prix d'efforts toujours croissants. Hunyadi poursuit ainsi :

> Le mode de vie représente la face sous laquelle le système se présente aux acteurs, en leur imposant des attentes de comportements déterminés. […] Ainsi, on attend d'eux qu'ils travaillent, qu'ils consomment, qu'ils sachent s'orienter dans un univers technologique; qu'ils utilisent les moyens de télécommunication; dans le milieu professionnel, on attend qu'ils soient performants, productifs, disciplinés, mais aussi évalués, comparés et, de plus en plus, autoévalués; notre existence prend toujours plus la forme d'un curriculum vitae, et il est attendu que notre commerce avec autrui se déroule dans le cadre du politiquement correct. Tout cela, et mille choses encore, visibles ou insidieuses, caractérisent nos modes de vie. (2015, p. 44-45)

Cette pression dont fait mention Hunyadi s'applique d'abord aux individus, mais l'injonction à avoir recours au numérique s'étend également aux entreprises privées et aux administrations publiques. L'économiste et président du Forum économique mondial Klaus Schwab prophétisait déjà en 2017 :

> Nous sommes à l'aube d'une révolution technologique qui va fondamentalement changer nos relations aux autres ainsi que notre façon de vivre et de travailler. Ces changements, dans leur importance, leur portée et leur complexité, ne ressembleront en rien à ce que l'humanité a pu connaître jusqu'alors. (2017, s. p.)

Le Gouvernement du Québec rappelle que les administrations publiques sont elles aussi soumises à ces pressions induites par le numérique :

> Influencées par les expériences numériques vécues avec le secteur privé, les attentes des citoyens envers les services publics sont de plus en plus élevées. […] Cette dernière doit utiliser le numérique pour pallier la complexité administrative

> découlant de l'étendue des services qu'elle offre, afin de proposer une expérience plus harmonisée et intégrée. (2021, s. p.)

Ainsi, on évoque l'importance de procéder à une transformation numérique (« digital transformation ») des organisations. Le terme de transformation numérique fait ici référence à l'« [e]nsemble des changements organisationnels et opérationnels que subissent une entreprise ou un organisme en intégrant de nouvelles technologies numériques à leurs activités » (OQLF, 2020b). C'est pour répondre à cet impératif de transformation numérique que le Gouvernement du Québec lançait en mars 2021 *l'Offensive de transformation numérique*, une stratégie pilotée par le ministère de l'Économie et de l'Innovation visant à soutenir financièrement les organisations désirant réaliser un projet de transformation numérique. (Gouvernement du Québec, 2022)

Derrière cette injonction à transformer numériquement l'entreprise privée ou l'administration publique se trouve une certaine logique d'accumulation informationnelle. L'exploitation de l'information sous forme de données est au cœur des technologies numériques. L'analogie entre la donnée et le pétrole est bien connue : la donnée serait à la nouvelle économie numérique ce que le pétrole a été pour la modernité. Pour tirer le plus de bénéfices possible des outils technologiques, et particulièrement de l'intelligence artificielle, il faut toujours davantage d'information, en quantité et en variété. La genèse de cette logique d'accumulation informationnelle remonte, selon plusieurs auteurs, à la triple convergence entre les travaux du mathématicien et cybernéticien Norbert Wiener, la science militaire et la contre-culture hippy des années 60 (Benoit, 2019; Breton, 1997; De Grosbois, 2018; Lafontaine, 2004; Sadin, 2016; Turner, 2006; Zuboff, 2015). L'historien israélien Yuval Noah Harari forge le néologisme « dataïsme » pour désigner cette posture théorique qui considère que la valeur d'un phénomène ou d'une entité est déterminée par sa « contribution au traitement des données » (2017, p. 395). Les auteurs vont désigner différemment ce phénomène lorsqu'ils l'envisagent du point de vue de son application aux phénomènes humains. Alors que la sociologue américaine Shoshana Zuboff parle du capitalisme de surveillance pour désigner l'appropriation de l'expérience humaine en tant que matière première pour la création d'outils de prédiction comportementale (2020, p. 8), Maxime

Ouellet de l'Université du Québec à Montréal lui préfère le terme de capitalisme cybernétique (2016, 2021). Finalement, les professeurs de sciences des communications Nick Couldry et Ulysses Mejias parlent plutôt de la « Datafication » (terme que je traduirais librement par « mise en données massives de la vie humaine ») (Couldry et Mejias, 2019a, 2019b, 2020; Sadowski, 2019) pour désigner la conversion de toutes les facettes de la vie humaine sous forme de données quantifiées visant à générer ultérieurement de la valeur pour les organisations qui les exploitent. Il s'agit ni plus ni moins pour eux d'une extension du capitalisme colonialiste qui, faute de nouveaux territoires physiques à exploiter, s'est trouvé un nouvel eldorado en l'exploitation de la vie humaine par le biais des technologies de l'information.

Cette logique d'accumulation informationnelle rejoint l'idée baconienne bien connue que l'information confère à son détenteur un certain pouvoir sur une entité ou sur un phénomène (Couldry et Mejias, 2020; Véliz, 2020). Le lien avec la protection de la vie privée émerge dès lors que l'on considère l'impact de cette logique informationnelle sur les individus. Comme le résume le professeur de droit américain Neil Richards : « Privacy is about power because information is power, and information gives you the power to control other people. » (2022, p. 42) Ce dernier rappelle dans son ouvrage *Why Privacy Matters* qu'il importe de protéger la vie privée non seulement pour préserver la dignité des personnes, pour favoriser leur autonomie ou pour défendre d'autres valeurs importantes, mais surtout pour contrer l'asymétrie de pouvoir que la collecte et l'utilisation de renseignements personnels confèrent aux entreprises, aux gouvernements et aux administrations publiques sur les consommateurs et les citoyens. Véliz ne dit pas autre chose :

> There is power in knowing, and knowledge in power. Power creates knowledge and decides what gets to count as knowledge. Through collecting your data and learning about you, Google becomes empowered, and that power allows Google to decide what counts as knowledge about you through its use of your personal data. Through protecting our privacy, we prevent others from being empowered with knowledge about us that can be used against our interests. By having more power, we have more of a say in what counts as knowledge. (2020, p. 51-52)

Comme le rappelle le juriste et professeur de droit Daniel Solove, la référence orwellienne au *Big Brother* gouvernemental et à sa déclinaison pour le secteur privé, les *Little Brothers,* ne sont jamais très loin lorsqu'il est question de protection de la vie privée. La possibilité d'une surveillance ubiquitaire soulève bien souvent les craintes et les interrogations. Pour ajouter aux références littéraires, Solove invoque également *Le Procès* de Kafka. Dans un univers social marqué par une gouvernance assumée furtivement par la collecte et le traitement en continu des données, le citoyen ou le consommateur moyen peut en effet vivre un désarroi similaire à celui vécu par le protagoniste du roman dystopique tout au long de son procès, alors qu'il est maintenu dans l'ignorance quant au crime qu'il aurait soi-disant commis et sans pouvoir y faire quoi que ce soit (Solove, 2001).

La transformation numérique des organisations et le mode de vie qui en découle sont dans une boucle de rétroaction alimentée par cette logique d'accumulation informationnelle. L'accélération de la mise en chantier de systèmes informatiques visant à répondre aux exigences de la transformation numérique engendre un mode de vie qui renforce, en retour, le besoin de mettre en place de nouvelles solutions numériques. Or, ce triplet « mode de vie/transformation numérique/logique d'accumulation informationnelle » ne semble pas tout à fait compatible avec la protection de la vie privée. En effet, à l'ère des objets connectés, des ensembles de mégadonnées et de l'exploitation tous azimuts de l'information par des algorithmes d'intelligence artificielle, la protection de la vie privée prend souvent l'allure d'un frein à l'innovation. La protection de la vie privée passait déjà souvent au deuxième plan derrière les considérations de sécurité publique et de sécurité nationale. Désormais, elle se retrouve dans un environnement qui fait reposer l'innovation sur l'utilisation massive de renseignements et, corollairement, des renseignements personnels.

Alors que les administrations publiques et les entreprises privées sont en quelques sortes forcées de se transformer numériquement pour des raisons de gestion efficiente de fonds publics, de compétitivité ou d'attractivité, elles subissent concurremment de la pression pour accorder une attention croissante à la protection de la vie privée de leurs communautés ou de leur clientèle. C'est dans ce contexte que les gouvernements sont pressés d'adopter des

législations modernes permettant de garantir une certaine protection face à l'effritement des frontières de la vie privée provoqué par l'augmentation exponentielle des capacités de collecte et de traitement des renseignements personnels et par l'intrusion toujours plus profonde des technologies numériques dans le quotidien et dans l'intimité. Pour répondre aux limites du modèle traditionnel de protection de la vie privée qui misait principalement sur l'autonomie informationnelle des personnes, notamment sur le consentement et la possibilité d'exercer des droits individuels, les nouvelles obligations visent à renforcer la responsabilisation des organisations. Ainsi, les organisations sont appelées à se réguler elles-mêmes dans la mise en œuvre de leurs projets informatiques impliquant des renseignements personnels. Or, comme le laissent entrevoir les trois citations en exergue, le consensus sur la nature, l'étendue et la valeur de la protection de la vie privée n'est pas gagné d'avance. L'existence même de l'objet « vie privée » est parfois remise en question.

Une nouvelle obligation : l'évaluation des facteurs relatifs à la vie privée

En raison de l'obsolescence de ses lois face aux nouveautés technologiques, le législateur québécois a jugé important d'introduire un certain nombre de nouvelles obligations en matière de protection des renseignements personnels pour les organismes publics et pour les entreprises du secteur privé. La sanction en septembre 2021 de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ [2021]. c. 25, la « Loi 25 ») — également connue sous la dénomination de « projet de loi no 64 » — est venue modifier ou ajouter plusieurs dispositions prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, la « Loi sur l'accès ») et à la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, chapitre P-39.1, la « Loi sur le privé »).

Il est fait mention à quelques reprises de nouvelles obligations visant la réalisation d'un processus désigné par le terme d'*évaluation des facteurs relatifs à la vie privée* (ÉFVP). L'une des situations où les organisations publiques et les entreprises du secteur privé auront à produire une telle évaluation est d'intérêt dans le contexte de la transformation numérique.

À partir de septembre 2023, tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels devra faire l'objet d'une ÉFVP (article 63.5 de la Loi sur l'accès[1] et article 3.3 de la Loi sur le privé[2]). Alors que cette obligation est tout à fait nouvelle pour les entreprises du secteur privé, les organismes publics devaient déjà, dans certains cas, produire une évaluation qui s'y apparente, et ce, en vertu de l'article 7 du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r.2)[3].

Signalons d'emblée que l'obligation de réaliser une ÉFVP (ou de réaliser une évaluation qui lui est apparentée) n'est pas le propre du Québec. Dans les faits, la pratique de faire un *Privacy Impact Assessment* (ou PIA) remonte aux années 70 (Clarke, 2009). Ainsi, le PIA est obligatoire pour les agences fédérales aux États-Unis depuis 2002 en vertu du *E-Government Act.* Une telle obligation existe déjà pour les organisations relevant du gouvernement fédéral canadien depuis 2011, et ce, en vertu de la *Directive sur l'évaluation*

[1] « 63.5. Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. […] La réalisation d'une évaluation des facteurs relatifs à la vie privée en application de la présente loi doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. » (CAI, 2022c)

[2] « 3.3. Toute personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. […] La réalisation d'une évaluation des facteurs relatifs à la vie privée en application de la présente loi doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. » (CAI, 2022b)

[3] « Un organisme public doit informer le comité visé à l'article 2 des projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels. Le comité suggère, parmi ces projets, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels. Ces mesures comprennent : […] 2° l'évaluation, dès l'étude préliminaire du projet, des risques d'atteinte à la protection des renseignements personnels; 3° des mesures propres à assurer la protection des renseignements personnels pendant toute la période de réalisation du projet et son maintien lors de l'utilisation, de l'entretien, de la modification et de l'évolution du système d'information ou de prestation électronique des services visés; […]. »

des facteurs relatifs à la vie privée du Secrétariat du Conseil du trésor fédéral[4]. Depuis l'entrée en vigueur en 2018 du *Règlement général sur la protection des données* (mieux connu sous l'acronyme RGPD), l'Union européenne exige que les entreprises qui font commerce auprès des citoyennes et citoyens de ses États membres produisent une *analyse d'impact à la protection des données* (AIPD) pour tout projet susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Déjà en 2016, la Commission d'accès à l'information du Québec (CAI) faisait la recommandation d'obliger les promoteurs d'un projet impliquant d'avoir recours à des caractéristiques ou à des mesures biométriques à réaliser à un processus d'évaluation des risques et des préjudices portés à la vie privée et à la protection des renseignements personnels. Elle faisait également une recommandation similaire pour les communications de renseignements personnels susceptibles d'avoir un impact important sur la vie privée des personnes concernées (CAI, 2016, p. 105; 126). Bref, l'adoption de la loi 25 a permis de mettre le Québec au diapason d'autres législations sur ce point plus précis.

Les lois étant ce qu'elles sont, elles donnent peu de détail concernant la procédure, le contenu attendu et les objectifs reliés à la réalisation d'une ÉFVP. Néanmoins, il existe suffisamment de précédents pour obtenir une idée générale de la nature de cet exercice. Une norme ISO portant sur les ÉFVP existe (Organisation internationale de normalisation, 2017) et de nombreux guides ont été produits par les organismes gouvernementaux de surveillance et de contrôle en matière de protection des renseignements personnels et de protection de la vie privée. En plus des guides réalisés par le Commissariat à la protection de la vie privée du Canada (CPVPC) et par la CAI (CAI, 2021; CPVPC, 2011), une courte recherche sur un moteur de recherche permet d'en retracer plusieurs autres. Au Canada, l'Alberta et la Colombie-Britannique ont également produit de tels guides et ceux des organismes de contrôles britanniques, néo-zélandais et australiens (province de Victoria) sont des exemples intéressants. En outre, les instances de l'Union européenne et les autorités de contrôle

[4] Notons toutefois que, contrairement aux entreprises assujetties à la Loi sur le privé qui devront produire des ÉFVP dès septembre 2023, les entreprises privées à charte fédérale en sont pour l'instant exonérées.

territoriales, comme la Commission Nationale de l'Informatique et des Libertés (CNIL) de France, ont également produit de nombreux outils intéressants pour orienter la réalisation des AIPD.

Il est généralement fait référence à deux objectifs pour la réalisation du processus d'évaluation présenté dans ces différents guides. Le premier concerne la démonstration de la conformité aux lois en matière de protection des renseignements personnels ou de protection de la vie privée. Le second répond à la volonté d'anticiper les risques et les préjudices potentiels qu'un projet portera à la vie privée des personnes concernées par sa mise en œuvre. Le présent mémoire s'intéresse plus spécifiquement à ce second volet.

Problématique et plan des chapitres

La volonté derrière la réalisation de ce mémoire a d'abord été pratique. Il s'agissait de voir comment outiller et accompagner les organismes publics et les entreprises du secteur privé en établissant une certaine cartographie des risques et des préjudices portés à la vie privée. Or, il est apparu très tôt dans la recherche que ces notions de risques et de préjudices portés à la vie privée s'avèrent très complexes. La volonté pratique du début s'est ainsi partiellement estompée pour laisser place à une réflexion animée par une perspective davantage critique. L'intention — fort louable par ailleurs — du législateur québécois de vouloir hausser le niveau de protection de la vie privée des Québécoises et des Québécois allait-elle véritablement s'incarner par la réalisation d'ÉFVP par les entreprises et les organismes publics? Dès lors, l'objectif général de ce mémoire fut d'explorer les conditions qui permettraient potentiellement de concrétiser les ambitions proclamées de ce genre de processus évaluatif du point de vue de l'éthique. Pour ce faire, je m'attarde d'abord à parcourir la nature des risques et des préjudices portés à la vie privée et des processus visant à les évaluer, ce qui inclue *de facto* les ÉFVP. Les premier et second chapitres de ce mémoire concernent plus spécifiquement ces notions. Les constats qui sont faits dans ces deux premiers chapitres me servent par la suite de mettre en relief dans le troisième chapitre quelques enjeux éthiques concernant le renforcement de la protection de la vie privée par la réalisation des ÉFVP.

Ainsi, la première question qui a guidé cette recherche est la suivante : en quoi consisterait une évaluation des risques et des préjudices portés à la vie privée réalisée pour un projet informatique qui se voudrait véritablement protectrice de la vie privée? Cette première partie de la recherche a été conduite avec deux questions en tête. Ces sous-questions ont présidé à la rédaction de mes deux premiers chapitres. Ainsi, le premier chapitre vise d'abord à dresser les grandes lignes des pourtours de ce que sont les risques et les préjudices portés à la vie privée (section 1.4). Avant d'y arriver, j'aborde cependant plus généralement les notions de protection des renseignements personnels (section 1.2) et de processus d'évaluation des risques (section 1.3) afin d'apporter un éclairage plus précis sur ce qu'une évaluation des facteurs relatifs à la vie privée pourrait contenir et devrait couvrir.

Le second chapitre est plutôt aiguillé sur la question « qu'est-ce que "protéger la vie privée"? » Il s'agit de faire un tour d'horizon des réponses contemporaines qui ont été données à cette question (section 2.2), de faire ressortir certaines des caractéristiques principales de l'objet « vie privée » — nommément sa multidimensionnalité (section 2.3.1), son caractère hautement contextuel (section 2.3.2) et sa potentielle *contestabilité essentielle* (section 2.3.3) — et de mettre en relief sa valeur instrumentale (section 2.4). Au final, ces deux premiers chapitres visent principalement à souligner la complexité qui semble exister pour ceux qui veulent articuler la protection de la vie privée sous forme de mécanisme d'évaluation. L'hypothèse de travail est qu'une évaluation des risques et des préjudices portés à la vie privée qui se voudrait véritablement protectrice de la vie privée est en fait l'équivalent d'une évaluation éthique du projet. Dans la mesure où l'argumentaire est valable, il faut considérer que la portion « vérification de la conformité » de l'évaluation des facteurs relatifs à la vie privée devrait être complétée par une évaluation des risques éthiques. C'est-à-dire que l'évaluation des risques doit inclure une évaluation des risques éthiques en plus d'une évaluation des risques juridiques ou des risques de sécurité de l'information. Une telle évaluation serait analogue à ce qu'on peut voir, par exemple, dans les processus d'évaluation éthique des projets de recherche avec les humains.

Le troisième chapitre fait l'esquisse de deux sujets plus proprement éthiques qui sont distincts, mais reliés. Dans la première partie (section 3.2), je conteste la possibilité de tenir une évaluation des risques qui tiendrait compte à leur juste valeur des risques et des préjudices portés à la vie privée. Ce questionnement s'appuie sur certaines caractéristiques que ces derniers présentent, notamment le fait qu'ils sont souvent peu préjudiciables (section 3.2.1), qu'ils concernent non seulement des individus, mais parfois des collectivités (section 3.2.2) et que leur matérialisation est fortement liée au contexte (section 3.2.3). Il s'agit d'entrevoir à quel point les risques et les préjudices portés à la vie privée peuvent avoir un véritable poids dans l'évaluation du rapport coûts/bénéfices d'une organisation qui se retrouve dans le contexte décrit en début de cette introduction. Par la suite, j'aborde brièvement la question corollaire des conditions de réalisation d'une évaluation des risques valable et impartiale. La première question soulevée concerne la prise en compte des risques et des préjudices portés à la vie privée dans un contexte d'évaluation basée sur une logique utilitariste (section 3.3.1). Pour finir, je survole la question de la posture professionnelle requise de l'évaluateur (section 3.3.2) et celle de la faisabilité de l'obligation de réaliser des évaluations des facteurs relatifs à la vie privée (section 3.3.3).

Précisions méthodologiques

Ce travail de recherche ne comprend pas de volet empirique. Il est principalement constitué d'un travail d'analyse conceptuelle à partir de sources bibliographiques. Il s'est avéré nécessaire de limiter le corpus à l'étude, car la documentation abordant la question de la vie privée est très abondante et foisonnante. Le tri a été à la fois disciplinaire, temporel et sociogéographique. Il a été disciplinaire d'abord, car la question de la vie privée n'est pas l'apanage d'une seule discipline académique : elle a été abordée selon des points de vue anthropologiques, historiques, juridiques, philosophiques, économiques, politiques, sociologiques et même psychologiques. Il a été temporel ensuite, car cette question est d'actualité depuis au moins l'Antiquité, sous une forme ou sous une autre (DeCew, 2018; Duby et Ariès, 1999). Finalement, il a été sociogéographique, car les réponses qui sont données à cette question sont fortement marquées par les contextes desquels elles émergent

(Nissenbaum, 2009). Ainsi, la présente recherche a été produite à partir de textes scientifiques provenant principalement des domaines du droit et de la philosophie, ainsi qu'à partir de certains documents issus de la documentation grise. Je me suis limité à consulter des écrits contemporains et occidentaux. Ce choix a été fait parce que l'exhaustivité ne m'a pas paru nécessaire ni même atteignable considérant que le sujet de la vie privée est largement débattu encore de nos jours. L'actualité de la question est criante et rares sont les journées où ne paraît aucun article scientifique ou article de presse qui touche de près ou de loin au sujet. Du reste, cette grande vivacité du sujet, la quantité et la variété impressionnante de la documentation appuient par la bande l'un des constats principaux de ma recherche, à savoir que la question de la vie privée est éminemment complexe et que l'évaluation des risques et des préjudices qui lui sont portés ne peut être que complexe elle aussi.

Deux mises en garde supplémentaire s'imposent également quant au corpus abordé. Les différents écrits qui portent sur la vie privée couvrent des registres qui s'apparentent, mais ne s'équivalent pas nécessairement. Ainsi, certains textes portent sur la notion même de « vie privée », d'autres s'intéressent au « droit *à la* vie privée » et d'autres encore sur le « droit *de la* vie privée ». Alors que les premiers s'intéressent à la question de ce qui constitue la vie privée (ses limites, son étendue, sa définition, etc.), les seconds vont porter sur les bases juridiques ou philosophiques justifiant la défense de celle-ci et les troisièmes vont s'attarder à décrire l'état du droit sur la question. La distinction entre les trois registres, et plus particulièrement entre les deux premiers, n'est pas toujours très claire et bien définie. Il est possible qu'une analyse très poussée de mes sources révèle certains glissements sémantiques inadéquats.

De plus, le risque de confusion s'accentue pour le locuteur francophone du fait que la plupart des textes contemporains importants ont été écrits en anglais. Or, il ne semble pas toujours évident que l'usage des termes « vie privée » en français et « privacy » en anglais couvrent une réalité sémantique totalement identique (Poulsen, 2019a, 2019b; Rey, 2012; Rossi, 2020). Cette problématique pourrait en soi faire l'objet d'un travail d'analyse important. Dans les faits, le terme « vie privée » peut traduire aussi bien le terme « private

life » que le terme « privacy ». Alors que « private life » renvoie davantage à l'aspect biographique de la vie d'un individu, « privacy » renvoie plutôt à l'idée que quelque chose est privé, est protégé ou soustrait de la connaissance ou de l'influence des tiers. En plus, dans certains cas, « privacy » devrait plutôt être rendu par « protection des renseignements personnels », car le texte en question fait plus précisément référence à l'aspect informationnel de la vie privée.

Malgré les risques d'erreur, comme il demeure assez commun de traduire « privacy » par « vie privée », je vais privilégier l'usage de cette expression, sauf dans les cas où « protection de la vie privée » ou « protection des renseignements personnels » me paraît rendre mieux l'idée de l'auteur ou de l'autrice anglophone. Pour m'assurer de respecter les termes communément utilisés au Québec, je privilégierai l'utilisation de l'expression « protection des renseignements personnels » pour désigner la protection de la dimension *informationnelle* de la vie privée. Ce terme peut également être entendu au sens de « protection des données personnelles », de « protection des données à caractère personnel » ou de toute autre appellation qui voudrait signifier la protection de la vie privée informationnelle. Finalement, l'expression « processus d'évaluation des risques et des préjudices portés à la vie privée » fait référence de manière générale à ces processus, alors que l'expression « évaluation des facteurs relatifs à la vie privée » fait spécifiquement référence au processus prévu d'évaluation dans les lois québécoises.

Il faut souligner que certains des documents consultés pour ce mémoire ont été publiés avant la sanction du projet de loi et n'ont pas été mis à jour au moment d'écrire ces lignes. Il paraît donc normal que persistent certaines différences ou imprécisions entre les obligations prévues dans les lois québécoises et dans la documentation produite sur le sujet. En outre, il faut considérer qu'il s'agit là de droit nouveau pour le Québec. L'expérience, la jurisprudence et les travaux des organismes publics et chercheurs impliqués dans ce domaine pallieront éventuellement les informations lacunaires. Finalement, faut-il rappeler que ce mémoire de recherche est réalisé dans une perspective éthique et non juridique, par une personne qui n'est pas juriste de formation de surcroît? En conséquence, même s'il est beaucoup question de

droit tout au long du texte, des erreurs de compréhension juridique peuvent très bien s'être glissées. Le cas échéant, ces dernières devront m'être attribuées. Je considère toutefois que ces potentielles erreurs n'auront que peu d'impact sur la réflexion plus proprement éthique. Néanmoins, je termine ces précisions en soulignant le caractère prospectif et théorique de ce mémoire. Je n'ai, pour cette raison, aucune prétention à l'exhaustivité ou à la vérité.

CHAPITRE 1
LES RISQUES ET LES PRÉJUDICES PORTÉS À LA VIE PRIVÉE

1.1 *INTRODUCTION*

Ce premier chapitre vise à présenter les processus d'évaluation des risques et des préjudices portés à la vie privée et à explorer les notions de risque et de préjudice employées dans le cadre de ces processus. J'entame ce chapitre par un bref survol de l'encadrement légal de la protection de la vie privée au Québec (section 1.2). Il me semble ensuite important de montrer à quel objet fait généralement référence l'expression « évaluation des facteurs relatifs à la vie privée » (ÉFVP) et de souligner sa spécificité par rapport à d'autres processus d'évaluation qui peuvent être réalisés dans le cadre de la mise en œuvre d'un projet technologique, soit l'évaluation de la conformité légale et la gestion des risques en matière de sécurité de l'information et de cybersécurité (section 1.3). Suivant ce survol, je poursuis sur la spécificité d'une telle évaluation qui réside dans la gestion des risques et des préjudices portés à la vie privée. Il semble ainsi important de me pencher sur les caractéristiques des notions de « risques et de préjudices portés à la vie privée ». Il paraît en effet essentiel d'en avoir une idée commune avant de tenir un exercice visant à les évaluer (section 1.4).

Ce premier chapitre vise trois objectifs. Le premier consiste simplement à définir les concepts mentionnés ci-dessus et qui seront repris tout au long des réflexions ultérieures. Il s'agit ensuite de mettre en relief certaines caractéristiques des notions de risques et de préjudices portés à la vie privée. Leur caractérisation me permettra de remettre en question leur portée dans un contexte d'évaluation des risques. Considérant que les évaluations des risques et des préjudices en général sont effectuées dans une perspective essentiellement utilitariste, c'est-à-dire qu'elle vise à minimiser les préjudices et à maximiser les bénéfices, les caractéristiques des risques et des préjudices portés à la vie privée — notamment le fait

que ceux-ci ont généralement peu d'impacts perceptibles lorsqu'ils sont considérés « à la pièce » — peuvent faire douter de l'utilité véritable des évaluations des risques et des préjudices.

Il s'agit finalement de mettre en place quelques éléments qui soulignent la complexité inhérente de la réalisation d'une ÉFVP. Tout processus d'évaluation des risques et des préjudices — comme le sont les processus d'évaluations des risques environnementaux, des risques financiers, des risques stratégiques, etc. — requiert un certain niveau d'expertise dans le domaine visé par ce processus. Or, l'ÉFVP réalisée dans un contexte technologique — si elle se veut véritablement protectrice de la vie privée des personnes concernées — nécessite de pouvoir s'appuyer sur un minimum de connaissances juridiques et technologiques spécialisées. Si l'analyse effectuée dans mon second chapitre s'avère adéquate, à ces compétences juridiques et technologiques devraient s'ajouter également des compétences en éthique. Ainsi, la complexité des processus d'évaluation et le niveau et la diversité des compétences nécessaires à leur réalisation me mèneront à poser des questions portant sur les conditions de leur réalisation, en considérant que leur qualité repose en grande partie sur les qualifications des évaluateurs.

1.2 *LA PROTECTION DE LA VIE PRIVÉE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

1.2.1 La protection des renseignements personnels au Québec

Coup sur coup élevé au rang de droit par la *Déclaration universelle des droits de l'homme* en 1948, dans la *Charte québécoise des droits et libertés de la personne* en 1976 puis, par dérivation, dans la *Charte canadienne des droits et libertés* en 1982, le droit à la protection de la vie privée s'est ensuite édifié et complexifié au Canada et au Québec par l'adoption de bon nombre de lois et de règlements. En effet, la couverture juridique du droit à la vie privée n'est pas garantie par une seule loi. La *Commission des droits de la personne et des droits de la jeunesse* (CDPDJ) le rappelle et elle en énonce les principales facettes [l'italique est de moi] :

> Si la notion de vie privée échappe à toute définition formelle en droit canadien, la Cour suprême en a esquissé les contours : celle-ci s'exprime à la fois en termes de *lieux*, *d'intégrité physique* et *d'information*, l'aspect informationnel de la vie privée se rapportant à la *confidentialité*, au *contrôle sur l'accès et l'utilisation* ainsi qu'à *l'anonymat*. La Cour d'appel du Québec, pour sa part, identifie comme composantes du droit au respect de sa vie privée le *droit à l'anonymat et à l'intimité*, le *droit à l'autonomie dans l'aménagement de sa vie personnelle et familiale* ainsi que le droit au *secret et à la confidentialité*. (2020, p. 34-35)

Au cœur des lois qui traitent de près ou de loin de la protection de la vie privée se trouvent les lois de protections des renseignements personnels. Ces dernières ont acquis une importance capitale en raison du rôle prépondérant que joue l'information au sein de la nouvelle économie fondée sur l'utilisation et l'exploitation des données. C'est pourquoi beaucoup d'attention leur a été accordée dans les dernières décennies.

La protection des renseignements personnels — PRP dans le jargon des spécialistes — est un ensemble de droits et d'obligations des entreprises ou des organismes publics qui sont liés à la gestion des renseignements personnels. Elle est la matérialisation juridique du volet informationnel de la protection de la vie privée. L'expression « protection des *données personnelles* » est plus souvent utilisée en droit européen. Malgré ces deux appellations différentes utilisées de part et d'autre de l'Atlantique, les mécanismes employés pour atteindre les fins visées par les différentes législations sont souvent apparentés.

Dans les dernières décennies, les législations européennes ont été généralement plus affairées en matière d'encadrement des renseignements personnels que les législations nord-américaines, notamment par l'adoption du *Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, désignée plus généralement par son diminutif de *Règlement général sur la protection des données* ou par son acronyme RGPD. Dans les dernières années, le Québec et le Canada ont voulu se mettre à jour en cette matière. Le gouvernement du Québec est passé à l'acte en sanctionnant en juin 2021 la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Au Canada, le

gouvernement libéral a déposé en novembre 2020 un premier projet de loi, le projet C-11 intitulé *Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois*. Ce dernier, mort au feuilleton en raison du déclenchement des élections à l'automne 2021, a été tout récemment ravivé en juin 2022 sous la forme du projet C-27 intitulé *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*. Plusieurs États américains se sont également dotés de lois plus modernes et plus robustes en matière de protection des renseignements personnels, comme la Californie l'a fait avec l'adoption du *California Consumer Privacy Act* en 2018.

Que faut-il entendre par la notion de « protection des renseignements personnels »? Denyse Roussell et Denis Bistodeau, auteurs du *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information pour les organismes publics*, la définissent ainsi :

> La protection des renseignements personnels constitue une des dimensions du respect de la vie privée. En principe, toute personne a un droit de regard sur les renseignements qui la concernent et qui peuvent être colligés, accessibles, utilisés, communiqués, conservés et détruits par un organisme public. Ces activités constituent les moments clés du cycle de vie des renseignements personnels. (2009, p. 6)

Paul-André Comeau, ancien président de la Commission d'accès à l'information du Québec (CAI), y va lui aussi de sa définition et énonce au passage le principe de finalité, ainsi que quelques droits qui lui sont associés :

> Ces lois [de protection des renseignements personnels] visent à assurer, aux différentes phases du cycle de vie d'un renseignement personnel, un traitement particulier. Elles régissent la production, la collecte, l'utilisation, la conservation, la circulation et éventuellement la destruction des renseignements personnels. Au cœur de ces modalités s'inscrit le principe de finalité qui soumet la détention de renseignements personnels à l'énoncé d'un objectif très précis et de celui-là

> seulement. Le régime de protection garantit aussi au citoyen un droit de regard sur les renseignements colligés et détenus à son sujet, en lui assurant notamment un droit d'accès et éventuellement de correction des données incomplètes ou erronées. (2012, p. 2)

Dans l'ensemble, la logique est la même : il s'agit de garantir une certaine protection aux personnes dans le traitement de leurs renseignements personnels tout au long du cycle de vie de ces derniers, c'est-à-dire de leur collecte (ou création) à leur destruction. Cette garantie s'appuie principalement sur l'autonomie des personnes à contrôler le flux des renseignements personnels qui les concernent (notamment par le biais du consentement) et par la responsabilisation des organisations qui collectent, utilisent et communiquent ces mêmes renseignements, en leur imposant par exemple une obligation de confidentialité et en les obligeant à mettre en place des mesures suffisantes en matière de sécurité de l'information et de cybersécurité. Ainsi, si la protection des renseignements personnels partage certaines considérations avec le domaine de la sécurité de l'information et de la cybersécurité, elle s'en distingue également du fait qu'elle s'attarde également aux considérations qui viennent en amont et en aval de la détention du renseignement personnel. Elle s'inscrit par ailleurs à l'intérieur de l'ensemble plus large qu'est le respect du droit à la vie privée qui lui ne se limite pas uniquement à des considérations de nature informationnelle.

Les mécanismes mis en place dans le contexte de la protection des renseignements personnels doivent également permettre aux personnes concernées d'exercer certains droits et certains recours en cas de mésusages des renseignements qui les concernent. Au Québec, cela comprend notamment :

- le droit d'une personne d'être informée des renseignements qu'une organisation détient à son endroit;
- le droit conféré aux personnes d'accéder aux renseignements qui les concernent et qui sont détenus par une organisation;
- le droit de voir ce renseignement être rectifié s'il est erroné;
- le droit de le voir être effacé lorsque sa conservation n'est plus requise.

Les processus de gestion et d'évaluation des risques et des préjudices à la vie privée — comme le sont les ÉFVP — font partie de la gamme d'outils administratifs et juridiques permettant aux organisations de démontrer leur sérieux quant à leur prise en charge des renseignements personnels et quant au respect de leurs obligations légales.

Les droits et les obligations applicables à la protection des renseignements personnels diffèrent selon les législations et selon la nature des entités impliquées dans le traitement des renseignements personnels. Ainsi, deux lois sont garantes de la protection des renseignements personnels au Québec. Pour les organismes publics[5], les obligations en cette matière sont édictées par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels des organismes publics* (RLRQ, chapitre A-2.1, la « loi sur l'accès »). Les entreprises du secteur privé[6] sont quant à elles régies par la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, chapitre P-39.1, la « loi sur le privé »). Un droit plus général au respect de la vie privée est enchâssé à l'article 5 de la *Charte des droits et libertés de la personne* (RLRQ, chapitre C-12) et le *Code civil du Québec* contient également certains articles qui concernent le droit à la vie privée. À l'instar du Québec, il existe deux lois fédérales qui couvrent la protection des renseignements personnels. Il s'agit de la *Loi sur la protection des renseignements personnels* (L.R.C. 1985, ch. P-21), qui concerne les organismes et ministères du gouvernement fédéral, et de la *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5), qui gouverne les entreprises du secteur privé. Contrairement à la charte québécoise, le

[5] Le terme « organisation publique » est entendu dans un sens très large qui couvre à la fois les ministères et les organismes publics, mais également les municipalités et les établissements des réseaux de l'éducation (centres de services scolaires, cégeps et universités) et de la santé (CIUSSS, CHSLD, hôpitaux, etc.). Cette énumération se trouve dans les articles 3 à 7 de la Loi sur l'accès.

[6] L'article 1525 du Code civil définit ainsi le terme « entreprise » : « Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services. »

droit à la vie privée n'est pas enchâssé explicitement dans la *Charte canadienne des droits et libertés*, mais y est reconnu par dérivation d'autres droits[7].

Ces lois tournent autour de la notion fondamentale de « renseignement personnel » (il est question en anglais de « Personal Identifiable Information » ou PII). Au Québec, les juristes utilisent deux définitions distinctes pour parler de renseignements personnels, bien que ces définitions soient très similaires en substance. La première se trouve à l'article 54 de la Loi sur l'accès et s'applique aux organismes publics visés par celle-ci : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier. » La seconde est édictée à l'article 2 de la Loi sur le privé et s'applique aux entreprises : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. » Il en va de même pour les lois fédérales qui prévoient deux définitions distinctes, mais qui sont similaires en substance au final. La définition de la *Loi sur la protection des renseignements personnels* encadrant les organismes publics définit le renseignement personnel comme étant tout renseignement qui, peu importe sa forme ou son support, concerne un individu identifiable. Cette définition est suivie par une liste non exhaustive d'exemples de renseignements visés par cette définition, comme les renseignements concernant l'appartenance ethnique d'une personne, sa religion, son âge, sa situation familiale, ses coordonnées, ses empreintes digitales, ses opinions, etc. Pour les entreprises du secteur privé visées par la *Loi sur la protection des renseignements personnels et les documents électroniques,* le renseignement personnel est « [t]out renseignement concernant un individu identifiable. » Pour sa part, le RGPD européen parle plutôt de « données à caractère personnel ». Dans tous les cas, comme le soulignent les professeurs Karim Benyekhlef et Pierre-Luc Déziel, la possibilité de rattacher un renseignement à un individu est le point commun entre ces différentes définitions. Ce qui

[7] D'autres lois sectorielles apportent nombre de précisions ou d'exceptions à toutes ces lois, notamment en ce qui concerne les renseignements de santé ou les renseignements fiscaux, mais leur recension exhaustive n'est pas pertinente dans le contexte de ce mémoire. L'ouvrage de Karim Benyekhlef et de Pierre-Luc Déziel intitulé *Le droit à la vie privée en droit québécois et canadien* est une source importante d'information à l'égard des lois québécoises et canadiennes encadrant la protection de la vie privée (Benyekhlef et Déziel, 2018).

permet de qualifier un renseignement de « personnel », c'est le fait qu'il est identifié à une personne (Benyekhlef et Déziel, 2018, p. 349). Ainsi, les obligations en matière de protection des renseignements personnels n'ont plus cours dès lors que les renseignements ne sont plus rattachés à des personnes physiques, comme le sont des statistiques par exemple ou des renseignements considérés comme étant dépersonnalisés ou anonymisés.

Il est à noter au passage que la législation québécoise en matière de protection des renseignements personnels fait mention explicitement du recours à l'éthique dans un cas bien précis : celui des sondages réalisés par un organisme public. En effet, le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r.2) oblige un organisme à consulter son comité sur l'accès à l'information et la protection des renseignements personnels pour évaluer, notamment, l'aspect éthique d'un sondage qu'une organisation prévoit de faire. Une telle obligation ne s'applique pas pour les entreprises du secteur privé. Avec la sanction de la loi 25, cette obligation se retrouvera désormais inscrite directement dans la Loi sur l'accès.

1.2.2 Quelques remises en question de la protection des renseignements personnels dans le contexte d'un recours massif au numérique

Le recours accru aux technologies numériques est venu ébranler certains principes derrière les mécanismes établis de protection des renseignements personnels. Au premier chef se trouve celui qui fait de l'identification le critère de qualification du renseignement personnel. L'importance architectonique du consentement pour la préservation de l'autonomie des sujets en est un autre.

Jusqu'à tout récemment, il pouvait sembler satisfaisant de « dépersonnaliser » le renseignement pour diminuer ou éliminer les risques qu'il soit lié de nouveau à une personne. Traditionnellement, la dépersonnalisation — le terme de « pseudonymisation » est aussi parfois utilisé — implique le retrait des renseignements qui sont directement identificatoires (par exemple, le nom et le prénom de la personne) ou indirectement (par exemple, une date

de naissance, un code postal ou même, dans certains cas, le diagnostic d'une maladie rare[8]). Le sujet des données est alors identifié par un numéro ou un identifiant quelconque. Selon le contexte d'utilisation, il est également possible d'envisager l'anonymisation des renseignements, c'est-à-dire de casser irrémédiablement le lien entre l'individu et le renseignement, ce qui est généralement fait par le biais de techniques de manipulation statistique avancées permettant d'établir que le renseignement a atteint un niveau d'anonymat suffisant. Dans les faits, les processus permettant une véritable anonymisation des données sont complexes, requièrent des compétences de statistiques avancées et génèrent beaucoup de mécompréhension de la part des personnes non expertes en la matière (EDPB et AEPD, 2021).

Comme le souligne Déziel (2018), les renseignements anonymisés échappent aux contrôles juridiques dans l'état actuel des choses du fait qu'ils ne correspondent plus au principe d'identification prévu dans les lois. De ce fait, ils seraient soustraits aux protections accordées aux renseignements personnels, même s'ils courent le risque d'être éventuellement personnalisés de nouveau. Selon les lois québécoises actuelles, un organisme public ou une entreprise privée doit détruire les renseignements personnels du moment que les finalités pour lesquelles ils ont été collectés ont été atteintes. Or, dès septembre 2023, de tels renseignements pourront être conservés si cette conservation est faite dans l'intérêt public (pour les organismes publics) ou pour des raisons légitimes (pour les entreprises privées), et ce, dans la mesure où ils auront été dûment anonymisés (CAI, s. d.). Le processus d'anonymisation en lui-même sera ainsi encadré, mais les renseignements sortiront quand même du champ d'application des lois dès lors qu'ils seront considérés comme étant anonymisés. Or, je le réitère, un renseignement qui pourrait paraître avoir été dûment dépersonnalisé ou anonymisé peut être réidentifié beaucoup plus facilement de nos jours en raison des grandes capacités de recoupement de l'information que permettent les algorithmes d'intelligence artificielle, de la puissance de calcul des processeurs et de la grande

[8] C'est pour éviter de révéler indirectement des renseignements personnels que les statisticiens vont parfois éviter de divulguer des données statistiques portant sur de petits nombres de cas.

disponibilité de renseignements variés sur les individus. Un renseignement que l'on ne considère plus comme étant « personnel » au moment X peut, selon le contexte, redevenir un renseignement dit « personnel » au moment Y s'il est croisé avec un ou plusieurs autres renseignements qui permettent de rétablir les liens entre eux et la personne qu'elles concernent. En fait, il apparaît peu prudent de déclarer un renseignement anonyme de façon permanente à l'exclusion peut-être des renseignements fortement agrégés comme des renseignements purement statistiques. Ainsi, l'anonymisation et, à plus forte raison, la dépersonnalisation des renseignements ne permettent plus de garantir hors de tout doute que la vie privée des personnes concernées soit protégée. La détermination du renseignement personnel sur la base du critère d'identification demeure donc sujette à discussion. En plus, Déziel et la Commission de l'éthique en science et en technologie (CEST) rappellent que les risques à la vie privée ne surviennent pas uniquement du fait qu'une personne est dûment identifiée (CEST, 2020b; Déziel, 2018). Un exemple d'une telle situation durant la pandémie fut le refus d'accès à un lieu public sur la base de la prise de température d'une personne. Dans cette situation précise, il n'y a nul besoin de connaître formellement l'identité de la personne concernée pour restreindre sa liberté de mouvement (le refus d'entrer dans un lieu public) en raison de la collecte et de l'utilisation d'un renseignement personnel (sa température corporelle). Pour répondre à ce genre de situation, Anna Johnston propose de substituer le critère *d'identification* de la personne par celui *d'individuation* :

> This paper uses the word individuation to refer to the ability to disambiguate or "single out" a person in the crowd, such that they could, at an individual level, be tracked, profiled, targeted, contacted, or subject to a decision or action which impacts upon them—even if that individual's "identity" is not known (or knowable). (2020, p. 10)

Au-delà de ces considérations portant sur la nature des renseignements visés par les lois, le principe du consentement, qui est pourtant au cœur de plusieurs mécanismes juridiques, est lui aussi malmené par le contexte technologique. Pour Neil Richards, l'idée que l'on puisse exercer un contrôle véritable sur toutes les utilisations qui sont faites de nos renseignements personnels par le biais du consentement relève du mythe dans le contexte des technologies de l'information. D'abord, il considère que la gestion des renseignements est

une tâche accablante pour le commun des mortels considérant le nombre d'interactions que nous avons quotidiennement avec des systèmes informatiques. Cette gestion par le consentement — qui doit être manifeste, libre et surtout éclairé pour être valide — relève, selon lui, de l'illusion, car les différentes technologies sont trop complexes et ramifiées afin de permettre à la personne un contrôle effectif du flux des informations générées à son sujet. Le contrôle individuel demeure insuffisant dans un univers où l'information est ubiquitaire et générée *par* tous et *au sujet de tous* et *de tout*. Dans les faits, Richards considère que le consentement rassure de façon erronée le consommateur par rapport aux effets autrement délétères et sinistres que génèrent les atteintes à la vie privée (2022, p. 90-100). D'autres auteurs remettent en question la valeur ou l'utilité du consentement dans le contexte actuel, notamment par Hartzog qui s'associe à Richards pour décrire le consentement comme étant un outil surutilisé et désormais inapproprié (Richards et Hartzog, 2019) et par Déziel, qui rappelle que l'« idée que les personnes éprouvent d'importantes difficultés à exercer un contrôle efficace sur leurs renseignements personnels dans les environnements numériques n'est ni nouvelle ni complètement étrangère au droit canadien. » (2018, p. 842)

Le juriste et professeur de droit américain Daniel J. Solove identifie lui aussi trois limites au droit à la protection des renseignements personnels opérationnalisé par l'octroi de droits distincts aux individus (Solove, 2022). Pour lui, l'addition de plusieurs droits distincts ne vient pas nécessairement renforcer l'autonomie des personnes. D'abord, il considère comme Richards que l'exercice de ces droits constitue un *fardeau interminable de corvées* (« an endless burden of chores »). Selon lui, la plupart des personnes n'ont ni le temps nécessaire ni les connaissances requises pour mettre en œuvre ces droits de façon effective. En effet, il peut paraître illusoire de penser qu'une majorité de personnes sont en mesure de lire et de comprendre l'ensemble des politiques de confidentialité qui leur sont présentées, qu'elles peuvent configurer adéquatement tous les paramètres de protection de la vie privée des appareils numériques et des applications qu'elles utilisent ou qu'elles prennent soin de bien connaître tous les méandres dans lesquels leurs renseignements personnels vont transiter. Il évoque ensuite le fait que l'exercice d'un droit est conditionnel au fait qu'une personne concernée connaisse l'existence de ce droit et, le cas échéant, qu'elle perçoive les

risques d'atteinte à celui-ci. La personne concernée doit avoir un niveau de connaissance et de compréhension suffisante des enjeux en sa présence pour ressentir la nécessité d'exercer un droit. Pour reprendre les exemples cités précédemment, il faut supposer qu'une personne a les compétences nécessaires pour déchiffrer le jargon utilisé dans les politiques de confidentialité, pour comprendre le véritable fonctionnement des paramètres de protection de la vie privée d'une application ou d'un appareil et pour bien saisir le circuit des renseignements personnels qui les concernent. Elle doit, en outre, appréhender les implications soulevées potentiellement par tous ces éléments. Je reviens d'ailleurs plus en détail sur ce dernier point au troisième chapitre, et particulièrement à la section 3.2.1. Finalement, pour Solove, l'exercice individuel des droits ne permet pas de rendre compte de la dimension collective et sociétale des problématiques engendrées par le recours aux renseignements personnels. Solove rappelle que la protection de la vie privée joue un rôle instrumental dans la défense de certains intérêts collectifs, alors que les renseignements personnels peuvent être utilisés pour agir sur des groupes ou des sociétés entières. À titre d'exemple, l'implication de la firme britannique Cambridge Analytica dans les élections américaines de 2016 et dans le Brexit a soulevé d'importantes questions concernant les possibilités de manipuler l'opinion publique à partir de renseignements personnels. Solove souligne également que les renseignements personnels sont souvent rattachables à plus d'une personne. Par exemple, un renseignement génétique peut être partagé par une fratrie entière. Des renseignements peuvent être affiliés à tous les membres d'une même famille, comme le sont des coordonnées. Finalement, Solove rappelle que les algorithmes d'intelligence artificielle ont désormais les capacités d'engendrer des effets sur de tierces personnes bien plus facilement à partir d'un jeu de données qui, parfois, pourrait en contenir très peu à leur sujet. Je reviens également plus en détail sur l'aspect instrumental et sur la dimension collective de la vie privée aux sections 2.4 et 3.2.2. Pour toutes ces raisons, Solove conclut que les droits octroyés aux individus ne permettent plus de garantir que leur vie privée soit adéquatement protégée.

Cette digression sur les limites de certains principes sur lesquels s'appuient les lois de protection de renseignements personnels met en lumière certaines raisons qui ont mené à la

mise en place des évaluations des facteurs relatifs à la vie privée. Comme le risque porté à la protection de la vie privée n'est pas forcément éliminé lorsque des renseignements utilisés ne sont pas « personnels », et parce que le consentement et l'idée qu'il est possible d'exercer un contrôle sur le flux des renseignements personnels relèvent plus du mythe que de la véritable possibilité, les législateurs, comme l'Union européenne et le Québec, ont cru bon de miser davantage sur la responsabilisation des organisations. Ainsi, cette volonté de responsabiliser les organisations — qui devront faire la démonstration d'une prise en charge minimale des considérations de protection de la vie privée — s'incarne notamment par la réalisation des ÉFVP.

1.3 *L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE*

1.3.1 Définir l'évaluation des facteurs relatifs à la vie privée

Concrètement, qu'est-ce qu'une ÉFVP? Bien qu'elles se recoupent sur certains points, les lois et la documentation existantes ne fournissent pas de vision consensuelle de ce qu'elle est. Malgré tout, je peux affirmer qu'il s'agit essentiellement d'un processus administratif ou juridique qui vise à évaluer « un projet » ou une « initiative » du point de vue de la protection des renseignements personnels ou de la protection de la vie privée au sens large. Pour la CAI, le terme « projet » vise une réalité très diversifiée et doit s'entendre de multiples façons. Un projet peut être : la mise en place d'un nouveau système informatisé (par exemple, un nouveau site Internet transactionnel), un système de prise de décision automatisée (par exemple, un outil qui détermine automatiquement le coût d'une prime d'assurances à partir de certains critères), la mise sur pied d'un nouveau programme gouvernemental, le démarchage d'une nouvelle clientèle pour une entreprise, l'utilisation secondaire de renseignements personnels pour tenir des projets de recherche, etc. (CAI, 2021, p. 3) Le Commissariat à la protection de la vie privée du Canada (CPVPC) et le Secrétariat du Conseil du trésor fédéral préfèrent utiliser les termes « programmes » et « activités » pour désigner les situations touchées par l'obligation de produire une ÉFVP (CPVPC, 2011; SCT-TBC, 2010). Du côté européen, le RGPD privilégie la notion de « traitement » pour désigner les

processus qui doivent faire l'objet d'une analyse d'impact relative à la protection des données (AIPD), l'équivalent en droit européen d'une ÉFVP. Selon l'article 4 du RGPD, le terme « traitement » désigne « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel ». Par commodité, et sauf indication contraire, j'utiliserai désormais le terme générique de « projet » pour désigner ce dont l'ÉFVP doit faire son objet.

Généralement, l'objectif de l'ÉFVP sera de démontrer que l'organisation a considéré toutes les facettes du projet susceptibles d'avoir un impact sur la vie privée des gens. Il est souvent fait référence à deux composantes de cette évaluation. La première consiste en la vérification de la conformité aux lois applicables en matière de protection des renseignements personnels et de protection de la vie privée. La seconde vise à identifier, gérer et mitiger ou éliminer les risques d'atteinte à la vie privée. L'ÉFVP vise donc deux sous-objectifs distincts, soit la conformité légale et la minimisation des risques et des préjudices portés à la vie privée. Ces deux éléments concourent à l'objectif principal, celui de protéger la vie privée des personnes concernées.

Le principe de *Privacy by design* proposé par Ann Cavoukian (2011), experte en protection de la vie privée et ancienne Commissaire à l'information et à la vie privée de l'Ontario, est souvent évoqué lorsqu'il est question d'ÉFVP. Le *Privacy by design* — terme traduit par *protection des renseignements personnels (ou de la vie privée) dès la conception* — est un cadre de référence bien connu des spécialistes du domaine de la protection de la vie privée. Ce dernier présente sept principes à appliquer pour tout processus de gestion ayant recours à des renseignements personnels. Ces principes sont :

- *Être proactif et non réactif, être préventif et non correctif (« Proactive not Reactive; Preventative not Remedial »).* Les mesures à mettre en place doivent viser plutôt à prévenir les risques et les préjudices à la vie privée plutôt qu'à les corriger. Il s'agit d'agir en amont sur les causes des problèmes plutôt que sur les effets.

- *La vie privée comme paramètre par défaut (« Privacy as the Default Setting »).* Les paramètres de protection de la vie privée les plus élevés sont toujours appliqués par défaut, l'utilisateur ayant par la suite l'occasion de choisir des paramètres moins protecteurs[9]. Parfois, ce principe est promu dans le titre du cadre de référence qui devient *Privacy by Design and by Default*.

- *La protection de la vie privée intégrée dès la conception (« Privacy Embedded into Design »)*. La protection de la vie privée est considérée dès les premières phases de conception des projets ou les premières réflexions entourant l'élaboration de nouvelles pratiques organisationnelles.

- *La protection de la vie privée comme jeu à somme positive, et non à somme nulle (« Full Functionality—Positive-Sum, not Zero-Sum »)*. La protection de la vie privée ne doit pas être considérée comme étant un frein ou un obstacle à l'atteinte des objectifs et des intérêts des parties prenantes, mais plutôt comme une situation de type « gagnant-gagnant », la recherche d'un compromis acceptable valant davantage que la mise en opposition des intérêts de chacun.

- *Assurer la sécurité de bout en bout (« End-to-End Security—Full Lifecycle Protection »)*. La sécurité des renseignements personnels doit être assurée à chacune des étapes de leur cycle de vie par des mesures administratives ou technologiques.

[9] Par exemple, au lieu de miser sur un consentement de type « opting-out » lors de la collecte de renseignements personnels, l'application de ce principe aurait pour effet de privilégier le mode « opting-in ». L'« opting-out » consiste à présumer le consentement. Les personnes concernées doivent plutôt signaler leur désistement. À l'opposé, le consentement explicite est demandé avant de procéder au traitement des renseignements personnels dans le mode « opting-in ». Dans un contexte technologique, cela s'exprime par exemple dans le fait qu'une application installée sur un téléphone communique par défaut les renseignements personnels et requiert que l'utilisateur se rende dans les paramètres de sécurité pour désactiver ces fonctions (« opting-out ») plutôt que de demander le consentement à l'installation. L'installation de fichier-témoin (les « cookies ») sur un poste informatique à l'insu de l'Internaute relève de la même logique : il faut les désinstaller ou prévoir une protection logicielle pour ne pas qu'ils s'installent automatiquement. Le choix du design des interfaces peut également mener à induire l'utilisateur d'une application ou d'un site web en défaut, ce qui constituerait une dérogation à ce principe (LINC-CNIL, 2019).

- *Assurer la visibilité et la transparence (« Visibility and Transparency—Keep it Open »)*. Les pratiques relatives à la protection de la vie privée doivent miser sur la transparence et l'ouverture afin de favoriser la confiance et la responsabilisation des différents acteurs impliqués.

- *Protection de la vie privée centrée sur l'utilisateur (« Respect for User Privacy—Keep it User-Centric »)*. Les intérêts des personnes concernées sont au cœur des préoccupations en matière de protection de la vie privée.

L'application du *Privacy by Design* implique que ces principes ont été mis en œuvre tout au long du design du projet et de sa mise en production. Il faut également être en mesure de le démontrer. La réalisation de l'ÉFVP, qui relève elle-même en quelque sorte de l'application de ces principes, devrait idéalement pouvoir démontrer cette prise en compte.

La réalisation d'une ÉFVP peut viser des objectifs autres que la seule protection de la vie privée des personnes concernées par un projet. Vincent Gautrais et Nicolas Aubin en déterminent certains qui sont autant d'incitatifs à la réalisation d'une ÉFVP pour les organisations. Ces objectifs peuvent être de :

- démontrer la diligence de l'entreprise en cas de poursuite ou d'enquête;

- contrer certaines craintes des usagers puisqu'elle démontre l'importance accordée à la protection de leurs données;

- identifier les mesures nécessaires au respect des droits et règlements en vigueur et implémenter ces mesures;

- identifier comment se protéger des fautes, actions ou inactions en provenance des tiers contractants;

- identifier les besoins en matière d'implantation de mesures de sécurité;

- identifier les parties prenantes pouvant procurer un apport bénéfique au projet;

- identifier s'il est possible ou réaliste de mener le projet à bien tout en respectant la Loi et

- identifier la présence des incidents de confidentialité qui pourraient représenter un préjudice grave aux usagers. (2022, p. 8-9)

Les travaux d'analyse réalisés dans le cadre d'un tel processus d'évaluation donnent généralement lieu à la production d'un rapport qui peut être diffusé au public afin de rendre compte des considérations qui ont été portées à la vie privée. Ce rapport d'évaluation peut également jouer un rôle important pour éclairer le consentement des personnes qui seraient tentées de recourir au produit résultant du projet, qu'il s'agisse d'un programme gouvernemental, d'un système d'information, d'une application sur téléphone mobile, etc. La diffusion d'un rapport favorise les chances qu'une personne concernée ou intéressée par le projet puisse consentir de façon plus éclairée, s'exposant ainsi de façon volontaire aux risques subsistants (ou du moins, aux risques connus et identifiés dans le rapport d'évaluation). Il est d'ailleurs assez facile de trouver des exemples de tels rapports d'évaluation, particulièrement pour les projets gouvernementaux, car, pour des raisons de transparence envers la population, les gouvernements ont généralement l'obligation de rendre disponibles de tels documents. L'application Alerte Covid est un exemple récent d'un projet ayant fait l'objet d'une ÉFVP par le gouvernement canadien (Santé Canada, 2020).

1.3.2 Teneur et contenu des évaluations des facteurs relatifs à la vie privée

Le contenu attendu d'une ÉFVP variera, parfois de façon importante, entre les législations ou dans la littérature grise portant sur le sujet. Dans la norme ISO 29134 intitulée *Lignes directrices pour l'étude d'impacts sur la vie privée,* l'Organisation internationale de normalisation (l'ISO) définit ainsi l'ÉFVP :

> Processus global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des données à caractère personnel, dans le cadre plus large du système de management des risques d'un organisme. (2017, p. 2)

Elle établit plus loin un lien explicite entre les risques à évaluer et les normes et principes juridiques mis en place dans la législation où l'évaluation des risques et des préjudices doit être effectuée :

> Il convient que l'organisme utilise des outils et techniques d'identification des risques sur la vie privée qui sont adaptés à ses objectifs et ses aptitudes, ainsi qu'aux risques auxquels il est exposé. Il convient d'utiliser les principes juridiques en matière de protection de la vie privée applicables dans le pays où la solution sera déployée pour soutenir l'identification des risques de violation des données à caractère personnel. (2017, p. 17)

Pour le CPVPC, une « ÉFVP est un processus de gestion des risques qui aide les institutions à s'assurer qu'elles respectent les exigences de la loi et à déterminer l'incidence éventuelle de leurs programmes et de leurs activités sur la vie privée d'individus » (2011, s. p.). La CAI, quant à elle, propose la définition suivante :

> L'EFVP (sic) est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées. Ces facteurs sont : la conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient; l'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts; la mise en place de stratégies pour éviter ces risques ou les réduire efficacement. (2021, p. 6)

Du côté européen, le Groupe de travail « article 29 » sur la protection des données (le « Groupe de travail "article 29" »)[10] définit ainsi l'analyse d'impact à la protection des données (AIPD) dans ses lignes directrices :

> Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire

[10] En référence à l'article 29 de la *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* qui institue un groupe consultatif et indépendant qui conseille la Commission européenne sur l'application de cette directive qui a précédé l'adoption du RGPD.

> face. […] Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve. (2017, p. 4)

Finalement, le *United States Department of Justice* précise que :

> A PIA [Privacy Impact Assessment] is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. (Department of Justice, 2014, s. p.)

Bien que le contenu attendu d'une telle évaluation varie, la finalité suivante est généralement incluse : anticiper les risques (ou vulnérabilités) engendrés par une collecte, une utilisation ou une communication de renseignements personnels afin d'éliminer les chances qu'ils se concrétisent ou de mitiger les impacts qu'ils pourraient avoir sur la vie privée de personnes concernées.

Il peut sembler que l'ÉFVP se confonde avec d'autres processus reliés de près ou de loin à la protection de la vie privée. Roger Clarke dresse ainsi un portrait en négatif de l'ÉFVP en signalant en quoi elle se distingue de ces autres processus (2009, p. 124-125). Ainsi, pour lui, l'ÉFVP n'est pas l'équivalent :

- des *stratégies ou politiques organisationnelles* en matière de protection de la vie privée parce qu'elle s'effectue sur un projet en particulier plutôt que sur l'encadrement général d'une organisation en matière de protection de la vie privée;

- des *audits* de protection de la vie privée, parce qu'elle est conduite en amont, dès la conception des projets plutôt qu'en aval;

- de *seules analyses de sécurité de l'information*, parce qu'elle doit s'intéresser à toutes les dimensions de la vie privée[11];

- des *analyses de risques internes ou des analyses de type coûts/bénéfices*, parce qu'elle doit tenir compte non seulement des intérêts de l'organisation et des partenaires, mais surtout de ceux des populations visés par le projet;

- des *vérifications de conformité légale*, parce qu'elle doit également tenir compte des attentes du public par rapport à la protection de la vie privée (de l'expectative de vie privée)[12];

- des *analyses de problèmes en matière de protection de la vie privée*, parce qu'elle doit s'attarder également à la mise en place de solution;

- des *énoncés généraux en matière de protection de la protection de la vie* privée, parce qu'elle doit être un processus évolutif par lequel l'organisation affine ses pratiques et adapte son design en matière de protection de la vie privée; et, finalement

- des *listes de contrôle ou de vérification* qu'un subalterne pourrait compléter, parce qu'elle nécessite l'assentiment des hautes autorités de l'organisation.

Ce portrait offert par Clarke permet déjà d'entrevoir la complexité de cet exercice qui ne doit pas être vu comme une simple formalité bureaucratique, mais comme un processus appliqué en contexte, anticipatif, global et effectué en continu.

[11] Les différentes dimensions de la vie privée sont abordées tout au long du chapitre 2, mais plus particulièrement à la section 2.3.1.

[12] L'aspect contextuel de la protection de la vie privée est abordé plus en détail à la section 2.3.2.

1.3.3 Spécificités des évaluations des facteurs relatifs à la vie privée produites pour des projets informatiques

Comme mentionné dans l'introduction générale de ce mémoire, des obligations de produire des ÉFVP pour certaines catégories d'initiatives impliquant des renseignements personnels se retrouvent dans la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Ces obligations s'appliquent tant pour les organisations publiques que pour les entreprises du secteur privé.

Sans trop entrer dans les spécificités juridiques, la loi obligera les organismes publics et les entreprises privées à réaliser une ÉFVP dans un certain nombre de situations dès septembre 2023. Ainsi, les organisations publiques devront effectuer des ÉFVP dans les situations suivantes :

> Lors d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels (article 63.5); Lorsqu'un organisme public souhaite collecter des renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune (article 64); Lorsqu'un organisme public veut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques (article 67.2.1); Lorsqu'un organisme public a l'intention de communiquer des renseignements personnels, sans le consentement des personnes concernées, conformément à l'article 68 de la Loi sur l'accès; Lorsqu'un organisme public veut communiquer, à l'extérieur du Québec, des renseignements personnels ou qu'il souhaite confier à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte de tels renseignements (article 70.1). (SRIDAIL, 2022, s. p.)

Les entreprises privées auront des obligations semblables, sauf pour les situations impliquant la collecte pour une organisation tierce ou pour les échanges de renseignements entre organismes publics. Elles auront donc à réaliser des ÉFVP lors d'un projet de système d'information ou de prestation électronique de service, avant de communiquer un renseignement personnel à l'extérieur du Québec et pour communiquer un renseignement

pour des fins d'étude, de recherche ou de statistiques sans le consentement de la personne concernée. Bien que ce mémoire s'intéresse plus spécifiquement à l'obligation de réaliser une ÉFVP pour les situations d'acquisition, de développement ou de refonte de systèmes d'information ou de prestation électronique de services impliquant des renseignements personnels, les considérations qu'il soulève peuvent sans doute s'appliquer aux autres catégories de projets visés par une telle obligation. Toutefois, chacune des catégories d'ÉFVP soulèverait probablement des enjeux distincts dont je n'entends pas faire l'inventaire.

La jurisprudence et la doctrine ou la publication éventuelle de ligne directrice par la CAI viendront sans doute préciser les réalités visées par les notions de « système d'information » ou de « prestation électronique de services ». À ce stade-ci, et en tenant compte de l'objectif de la loi 25, il paraît raisonnable de les interpréter le plus largement possible. Ainsi, selon l'Office québécois de la langue française (OQLF), l'expression « système d'information » fait référence à un :

> Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation. (2004)

Quant à elle, l'expression « prestation électronique de services » fait référence à toute « [p]restation de services gouvernementaux, sécurisés ou non, offerts aux citoyens par l'intermédiaire d'Internet » (OQLF, 2003). Malgré que cette définition fait directement référence aux services gouvernementaux, la Loi sur le privé utilisera aussi cette expression pour désigner les projets visés par cette obligation. L'obligation de réaliser des ÉFVP, tant pour le secteur public que pour le secteur privé, visera un nombre important de projets très diversifiés. Voici quelques exemples de projets qui seront vraisemblablement visés : la mise en place d'un site Internet transactionnel, le développement d'une application de téléphonie cellulaire, l'utilisation d'un système de surveillance appuyé par une technologie de reconnaissance faciale, la mise à jour d'une base de données, le rehaussement d'un système de traitement de demandes d'assurabilité impliquant un algorithme d'intelligence artificielle, etc.

Il est concevable qu'un projet de grande envergure ait plus d'une composante visée par l'obligation de réaliser une ÉFVP ou qu'une même composante soit visée par plus d'une obligation à réaliser une ÉFVP[13]. Par exemple, un projet d'une compagnie offrant des services financiers aux particuliers pourrait avoir comme objectif la mise en place d'un système visant à établir les montants des prêts basés sur un algorithme d'intelligence artificielle fourni par un prestataire de service offrant ses services en infonuagique. Ainsi, une ÉFVP devra être réalisée à la fois pour le système d'information en lui-même et pour le volet infonuagique qui impliquera fort probablement une communication de renseignements hors du Québec.

À cet égard, nous pourrions dire que le Québec va plus loin que le RGPD européen. L'obligation québécoise de produire une ÉFVP pour les systèmes d'information est de type « mur à mur ». Dès qu'il est question d'un tel projet, l'organisation publique ou l'entreprise privée (de la très petite entreprise à la multinationale) devra réaliser une ÉFVP[14]. Toutefois, du côté européen, l'obligation de produire une AIPD s'applique uniquement pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Neuf critères sont proposés par le Groupe de travail « article 29 » pour déterminer si un projet entre ou non dans cette catégorie (2017, p. 10-13). Ces neuf critères sont :

- La présence d'une fonction d'évaluation, de notation, de profilage ou de prédiction dans le système évalué;
- La présence d'un mécanisme de prise de décisions automatisée avec effet juridique ou effet similaire significatif;

[13] Les différentes obligations sont mentionnées à la page précédente.

[14] Il est important de mentionner à ce stade-ci que les lois prévoient une certaine modulation de l'envergure des ÉFVP. Je reviens sur ce sujet en page 42.

- La présence d'un traitement qui vise à observer, surveiller ou contrôler les personnes concernées, y compris par la collecte de données ou par une surveillance systématique d'un environnement accessible au public;
- L'utilisation de données sensibles ou à caractère hautement personnel;
- Le recours à une méthode de croisement de données ou de combinaison d'ensembles de données;
- L'utilisation de données concernant des personnes vulnérables (par exemple, celles concernant les enfants ou les minorités sexuelles);
- L'utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles (ce serait le cas lorsqu'il y a recours à la chaîne de blocs ou à l'informatique quantique par exemple);
- La mise en place d'un traitement qui, en lui-même, empêche les personnes concernées d'exercer un droit ou de tirer des bénéfices d'un service ou d'un contrat.

Pour le Groupe « article 29 », un projet répondant à l'affirmative à deux critères devrait normalement faire l'objet d'une AIPD. Il précise toutefois ceci :

> Plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD, quelles que soient les mesures que le responsable du traitement envisage d'adopter. (2017, p. 13)

En plus de ces neuf critères qui permettent d'établir des exemptions, les autorités de contrôle propres à chaque pays membre de l'Union européenne peuvent déterminer une liste de domaines d'affaires pour lesquels la réalisation d'une AIPD n'est pas obligatoire. À titre d'exemple, en France, la Commission Nationale de l'Informatique et des Libertés (CNIL) précise que l'analyse d'impact n'est pas obligatoire :

- quand le traitement figure sur la liste des exceptions adoptée par la CNIL après consultation du CEPD (Comité européen de protection des données) ;

- quand le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées ;

- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une AIPD a déjà été menée;

- quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (article 6 du RGPD), sous réserve que les conditions suivantes soient remplies :

    - qu'il ait une base légale dans le droit de l'UE [Union européenne] ou le droit de l'État membre;

    - que ce droit réglemente cette opération de traitement;

    - et qu'une AIPD ait déjà été menée lors de l'adoption de cette base légale. (CNIL, 2019, s. p.)

Ainsi, l'obligation de produire une AIPD est restreinte dans l'Union européenne alors que l'obligation québécoise est, pour l'instant du moins, universelle.

Bien qu'elle énonce des attentes spécifiques pour certaines situations où l'ÉFVP est requise, la loi québécoise demeure toutefois vague quant au contenu et aux attentes liées aux ÉFVP produites pour les situations impliquant un système d'information ou une prestation électronique de service. À titre d'exemple, la loi est plus précise quant à ses attentes pour les ÉFVP réalisées pour une communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques. Dans ce cas-ci, les lois prévoient que l'ÉFVP devrait permettre de conclure que :

> 1° l'objectif de l'étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées; 2° il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées; 3° l'objectif de l'étude, de la recherche ou de la production de statistiques l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation des

> renseignements sur la vie privée des personnes concernées; 4° les renseignements personnels sont utilisés de manière à en assurer la confidentialité; 5° seuls les renseignements nécessaires sont communiqués[15].

Ces objectifs pourront orienter les organisations et entreprises qui auront à réaliser des ÉFVP. Peu importe le moyen utilisé ou le processus favorisé, elles doivent être en mesure de démontrer qu'elles ont atteint ces objectifs.

Pour les ÉFVP liées aux projets de systèmes d'information, la Loi sur l'accès et la Loi sur le privé présenteront uniquement des critères permettant de moduler l'envergure du processus d'évaluation, sans préciser d'objectifs. Ces critères sont les suivants : « La réalisation d'une évaluation des facteurs relatifs à la vie privée en application de la présente loi doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. »[16] Il faut préciser que ces critères s'appliqueront aussi à toutes les autres obligations liées à la réalisation d'une ÉFVP. Le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité (SRIDAIL)[17] apporte la précision suivante :

> Par exemple, un petit projet de développement d'un système d'information impliquant des renseignements personnels qui ne sont pas considérés comme sensibles et qui sont en faible quantité pourra faire l'objet d'une évaluation des facteurs relatifs à la vie privée moins détaillée. Néanmoins, tous les aspects essentiels d'une bonne évaluation doivent être couverts. (2022, s. p.)

---

[15] Nouvel article 67.2.1 de la Loi sur l'accès (CAI, 2022c, p. 45) et version amendée de l'article 21 de la Loi sur le privé (CAI, 2022b, p. 25).

[16] Nouvel article 63.5 de la Loi sur l'accès (CAI, 2022c, p. 36) et nouvel article 3.3 de la Loi sur le privé (CAI, 2022b, p. 4).

[17] Le SRIDAIL est un secrétariat du ministère du Conseil exécutif du Québec dont l'une des missions est de « [s]outenir les ministères et organismes dans l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ainsi que des règlements adoptés en vertu de celle-ci » (SRIDAIL, 2021). Il était connu sous le nom de Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques (SAIRID) jusqu'à tout récemment, la responsabilité de la laïcité ayant été ajoutée à sa mission.

La question demeure toutefois : quels sont ces aspects essentiels d'une bonne évaluation? Comme je l'ai mentionné antérieurement, les deux composantes principales de l'ÉFVP sont généralement 1) la vérification de la conformité légale et 2) l'évaluation et la gestion des risques et des préjudices portés à la vie privée. Il semblerait peu probable que le législateur ait voulu que la qualité des vérifications de conformité aux lois soit modulée lors de la réalisation d'une ÉFVP. Le fait d'établir la « sensibilité » des renseignements concernés, la « finalité de leur utilisation », leur « quantité », leur « répartition » et leur « support » ne joue aucun rôle quant à l'applicabilité de la grande majorité des droits et obligations prévus aux lois de protection des renseignements personnels. Je fais référence ici, par exemple, à l'obligation de confidentialité, au droit à l'accès à l'information pour la personne concernée, à l'obligation de détruire les renseignements lorsque les finalités de son utilisation sont atteintes ou pour l'obligation pour une entreprise privée d'obtenir un consentement éclairé pour la collecte de renseignements personnels. Le critère juridique qui vise à établir cette applicabilité, c'est la nature du renseignement, soit celle d'être un « renseignement personnel ». Le renseignement personnel n'est pas moins confidentiel ou moins accessible du fait qu'il soit plus ou moins sensible ou qu'il soit porté sur tel support plutôt qu'un autre. Ainsi, quelle pourrait être la réponse à la question « qu'est-ce qu'il y a à moduler dans l'ÉFVP? » si ce n'est la composante « évaluation et gestion des risques et des préjudices portés à la vie privée »? Pour un projet dont les renseignements sont en apparence non sensibles, ou moins sensibles, ou peu nombreux ou répartis sur peu de supports, cette composante pourrait donc être minimale ou simplement tronquée.

Il est possible de critiquer certains de ces critères évoqués par les lois québécoises. Par exemple, pour Solove, la protection de la vie privée ne devrait pas être appuyée sur les caractéristiques des renseignements visés, par exemple leur sensibilité, et ce, pour deux raisons (Solove, 2008, p. 67-70). La première raison est qu'un renseignement n'est pas moins confidentiel parce qu'il est moins sensible, mais parce que son sujet (la personne concernée) le considère comme étant confidentiel ou parce qu'elle désire le conserver comme tel. Par exemple, une personne pourrait très bien vouloir — et avoir le droit de — garder pour elle son amour immodéré pour la musique du groupe de musique britannique Tears for Fears,

même si cette information paraît tout à fait anodine. À l'opposé, un renseignement très sensible, comme une condition médicale sévère, n'est plus confidentiel si la personne concernée la diffuse à un large public, par exemple sur les réseaux sociaux. Bref, la sensibilité du renseignement (ou son niveau de confidentialité) n'est pas une caractéristique essentielle de ce renseignement, mais est plutôt relative à la perception de la personne concernée par celui-ci[18]. La seconde raison est qu'un renseignement peu sensible en apparence peut, lorsqu'il est croisé avec d'autres, révéler une information beaucoup plus sensible. J'ai déjà souligné à la section 1.2.2 cette caractéristique des renseignements personnels alors que je relevais la difficulté de les anonymiser ou de les dépersonnaliser adéquatement à l'ère des mégadonnées et de l'intelligence artificielle. En outre, un renseignement qui apparaît peu sensible à un moment X dans le temps peut devenir très sensible à un moment Y. J'aborde plus spécifiquement cette deuxième situation dans la section 2.4.1.

En conclusion de cette section, je souligne que la mise en parallèle des textes juridiques et de la documentation portant sur les ÉFVP montre certaines contradictions sur la nature de l'exercice. L'ÉFVP est-elle un exercice uniquement juridique de vérification de la conformité du projet aux lois applicables? Est-elle une simple vérification des mécanismes de sécurité de l'information et de cybersécurité mis en place par le promoteur du projet? Ou devrait-elle être un exercice d'évaluation éthique visant notamment à identifier les impacts potentiels du projet sur la vie privée des personnes concernées et, plus largement, sur les risques et préjudices portés aux droits de la personne? Actuellement, la lecture de la documentation existante au Québec laisse croire que l'exercice sera vraisemblablement *juridique*, ce qui implique nécessairement l'aspect sécurité de l'information et cybersécurité, car il s'agit, comme je l'ai mentionné, d'une obligation légale de s'en préoccuper. Je pose toutefois l'hypothèse suivante dans ce mémoire : pour se révéler véritablement protectrice de la vie privée, une ÉFVP devrait comporter à la fois une évaluation juridique du projet, une évaluation du niveau de sécurité technologique dont jouissent les renseignements personnels

[18] L'aspect contextuel de la sensibilité du renseignement personnel est abordé plus en détail dans la section 2.3.2.

impliqués et une évaluation plus proprement éthique des risques et des préjudices portés à la vie privée des personnes concernées.

1.4 *LES NOTIONS DE RISQUES ET DE PRÉJUDICES PORTÉS À LA VIE PRIVÉE*

1.4.1 La notion plus générale de « risque »

En soi, la notion de « risque » apparaît assez simple à appréhender, le risque étant communément entendu dans le sens d'un « danger éventuel plus ou moins prévisible » comme le précise *le Petit Robert*. Toutefois, cette simplicité n'est qu'apparente, car le concept en lui-même, comme le mentionne Céline Kermisch, est difficile à appréhender et à définir. Il l'est ontologiquement d'abord, parce qu'il n'existe pas, il est potentiel et virtuel. Le risque qui se matérialise n'est plus un risque : il est un événement qui a eu lieu et qui a eu ses effets, souvent néfastes. Il est également difficile à saisir épistémologiquement, poursuit-elle, car le risque est un savoir sur quelque chose qui n'existe pas encore. Il est donc « un artefact construit par le sujet », le sujet étant la personne qui le définit : son évaluateur en l'occurrence (Kermisch, 2012, p. 3). Comment s'opérationnalise la considération de cette éventualité néfaste au sein d'un processus de gestion des risques?

Dans son *Vocabulaire de la gestion de risque*, l'OQLF définit ainsi le risque : « Probabilité que survienne un événement nuisible et éventualité qu'existe une menace plus ou moins prévisible pouvant influer sur la réalisation des objectifs d'une organisation. » Elle ajoute l'indication suivante :

> Les risques d'une organisation sont aussi bien politiques, économiques, financiers, sociaux, technologiques et stratégiques qu'informatiques, opérationnels ou organisationnels. Par exemple, lors de la réalisation d'un projet, le risque correspond à un événement dont la manifestation aurait une incidence sur au moins un de ses objectifs, comme le coût, le contenu, la qualité ou le délai du projet.

L'OQLF précise finalement que « [l]e terme *risque* est généralement utilisé lorsqu'il existe au moins la possibilité de conséquences négatives. S'il ne s'agit que de conséquences probables positives, on parlera plutôt de *possibilités* » (2020c, s. p.). Le terme « risque » a

donc une connotation négative : il s'agit généralement d'une éventualité qui causerait un préjudice pour la personne ou l'entité qui la subirait.

Pour Jean-Paul Louisot, le terme « risque » souffre d'une certaine ambiguïté et il lui préfère « vulnérabilité » pour désigner les événements potentiels aux incidences négatives et qui doivent faire l'objet d'une évaluation pour la gestion. Il propose « opportunité » pour désigner les événements dont la matérialisation engendrerait des effets bénéfiques pour une organisation (2014, p. 5). Pour lui, une vulnérabilité est caractérisée par trois paramètres, soit l'objet du risque, le péril et l'impact potentiel :

> Objet de risque : c'est la ressource qui est « en risque » […]. Péril : c'est l'événement aléatoire dont la survenance prive l'organisme d'une ressource partiellement ou totalement, de façon provisoire ou définitive. Impact potentiel : il s'agit, le plus souvent, des pertes financières induites, et plus généralement de l'impact sur l'atteinte des objectifs fondamentaux de l'organisme (tous ne sont pas traduisibles en termes financiers). La littérature préfère souvent le mot « gravité » qui suppose une traduction en termes financiers. (2014, p. 9)

L'ISO définit plutôt le risque comme étant l'« effet de l'incertitude sur les objectifs » (2018, s. p.), l'idée d'« objectifs » renvoyant généralement à une dimension stratégique ou financière. L'ISO précise qu'« [u]n effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces ». Ainsi, pour l'ISO, et contrairement aux autres points de vue rapportés plus haut, le risque n'est pas intrinsèquement négatif. L'organisme ajoute aussi que « [l]es objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux ». Finalement, pour l'ISO, un risque possède les caractéristiques suivantes : « Un risque est généralement exprimé en termes de *sources de risque* (3.4), *événements* (3.5) potentiels avec leurs *conséquences* (3.6) et leur *vraisemblance* (3.7). » La source de risque est entendue comme étant « tout élément qui, seul ou combiné à d'autres, est susceptible d'engendrer un risque ». L'événement est l'« occurrence ou [le] changement d'un ensemble particulier de circonstances ». La conséquence est l'« effet d'un événement affectant les objectifs ». La vraisemblance est la « possibilité ("likelihood") que quelque

chose se produise ». Sans surprise, on voit poindre là les grandes lignes de la plupart des processus d'évaluation des risques et des préjudices employés par les organisations.

En effet, cette définition qui fait du risque une « combinaison de la probabilité de l'occurrence d'un dommage et de la gravité de ce dommage » (International Electrotechnical Commission, 2013) se trouve derrière la plupart des processus d'évaluation des risques et des préjudices. Les organisations vont d'abord établir une liste des événements qui sont susceptibles d'arriver, généralement sous la forme de scénarios de risques[19]. Lorsque la recension de ces événements potentiels aura été réalisée, une évaluation de chacun de ces scénarios est effectuée. Cette évaluation est souvent faite à l'aide d'une matrice construite sur deux axes. Un premier axe permet d'estimer la gravité de l'impact (ou des impacts) de l'événement. Le second considère la probabilité de son occurrence. La figure 1 donne un exemple d'une telle matrice d'évaluation.

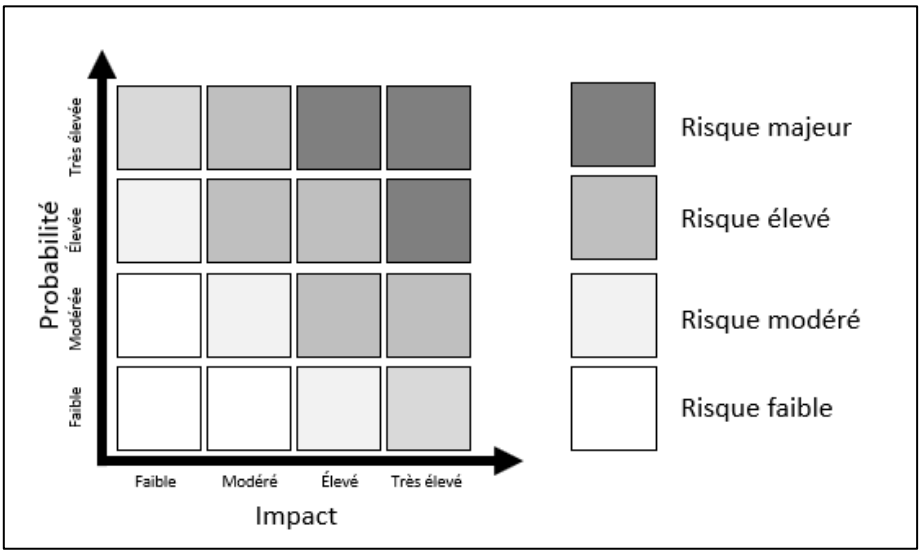

Figure 1. Matrice d'évaluation de risque.

[19] Il s'agit de la méthode proposée par le *Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité* (SRIDAIL) en 2006 dans un document qui présentait la méthode Méhari appliquée à la protection des renseignements personnels (Dionne, 2006, p. 12). Méhari signifie « méthode harmonisée d'analyse des risques ». Celle-ci fut d'abord implantée pour la gestion des risques en matière de sécurité de l'information.

Le croisement des deux valeurs se traduit dans une cote de risque qui permet de le mesurer objectivement et de déterminer si le risque est tolérable (le risque est faible ou modéré et le projet peut aller de l'avant sans modifications), inadmissible (le risque est élevé : sa probabilité de matérialisation doit être atténuée ou les impacts mitigés) ou insupportable (le risque est majeur, et le projet ne peut aller de l'avant tant que le risque subsiste) (Dionne, 2006, p. 10).

Il reste à l'évaluateur de décider s'il est à l'aise de vivre avec ce niveau de risque : il doit déterminer quel traitement il réservera au risque. Selon l'ISO :

> Le choix de la ou des options de traitement du risque les plus appropriées implique de comparer les avantages potentiels en termes d'atteinte des objectifs par rapport aux coûts, aux efforts et aux inconvénients de leur mise en œuvre.
>
> Les options de traitement du risque ne s'excluent pas nécessairement les unes les autres, et ne sont pas appropriées à toutes les situations. Les options de traitement du risque peuvent impliquer un ou plusieurs des éléments suivants :
>
> – un refus du risque marqué par la décision de ne pas commencer ou poursuivre l'activité porteuse du risque;
>
> – la prise ou l'augmentation d'un risque afin de saisir une opportunité;
>
> – l'élimination de la source de risque;
>
> – une modification de la vraisemblance;
>
> – une modification des conséquences;
>
> – un partage du risque (par exemple par le biais de contrats, de souscription de couvertures d'assurance);
>
> – un maintien du risque fondé sur une décision éclairée. (2018, s. p.)

Ainsi, si un risque est considéré comme étant trop grand par rapport à l'opportunité que représente le projet, il appartient à l'organisation de mettre en place des mesures visant à diminuer la gravité des impacts ou à réduire la probabilité de son occurrence, voire à

l'éliminer carrément. Comme le souligne Bernard Dionne (2006, p. 13-14), ces mesures peuvent être de différentes natures et vont agir soit sur les causes du risque (sur l'événement lui-même) ou sur les conséquences (sur l'impact du préjudice). Elles peuvent être structurelles (c'est-à-dire qu'elles « agissent sur la structure même du ministère ou de l'organisme public pour éviter qu'elle subisse certaines agressions de nature humaine ou autre, et pour en limiter la gravité, le cas échéant »), dissuasives (en vue de réduire les chances qu'un agent externe agisse malicieusement sur le projet), préventives (pour « empêcher une menace d'atteindre des ressources »), protectrices (pour limiter l'ampleur des préjudices), palliatives (pour réduire les impacts indirects du risque) et récupératrices (c'est-à-dire qu'elles visent à « récupérer une partie du préjudice subi en faisant endosser des pertes par des tiers [assurances, dommages et intérêts consécutifs à des actions en justice] »). Si le risque en évaluation n'est pas éliminé par la mise en place des mesures, il appartient à l'évaluateur de le réévaluer à la lumière des nouvelles mesures et voir s'il peut désormais tolérer le niveau de risque résiduel.

Ainsi, le processus d'évaluation des risques et des préjudices s'appuie sur un présupposé : celui qu'il est possible d'agir positivement sur des situations potentielles soit en amont (de manière préventive), soit en aval (pour réduire l'impact des préjudices vécus par les personnes concernées) par la mise en place de mesures adéquates. En d'autres mots, la Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST) :

> Le risque dénote la possibilité qu'un état indésirable de la réalité (effets défavorables) ne survienne à la suite d'événements naturels ou d'activités humaines. Cela signifie que les humains établissent des relations de causalité entre des actions (ou événements) et leurs effets et que les effets indésirables peuvent être évités ou atténués si les événements ou actions qui en sont la cause sont évités ou modifiés. (COMEST, 2005, p. 28)

La recension des définitions de la notion de « risque » à partir de la documentation portant sur la gestion de risques pourrait se poursuivre encore longtemps, mais nous en avons déjà les éléments les plus constitutifs. Je propose de la résumer ainsi : le risque est a) un

événement (une cause, un péril) b) d'une certaine nature (par exemple, économique, financier, social, politique, environnemental, etc.) c) qui a le potentiel de se matérialiser, selon des probabilités variables, et qui, s'il se matérialise, d) causerait un ou plusieurs préjudices d'intensité variable à e) une entité ou une catégorie d'entités (le sujet du risque).

Pour Kermisch, ces définitions qui font du risque une mesure des dommages potentiels s'inscrivent dans un paradigme quantitatif. Pour elle, les définitions tirées de ce paradigme — paradigme bien établi dans les processus de gestion des risques — sont pertinentes et utiles, car elles permettent d'appuyer la prise de décision dans un contexte où ces décisions doivent être légitimées par une certaine expertise, en s'appuyant notamment sur des données probantes et des démonstrations rigoureuses. En outre, les processus d'évaluation peuvent, dans un tel contexte, être réalisés par le biais d'outils bien définis, comme la matrice d'évaluation présentée précédemment. Ces définitions n'en seraient pas moins incomplètes selon Kermisch, car il est également possible d'aborder la notion de risque d'un point de vue qualitatif. Ce point de vue qualitatif est une conception constructiviste du risque :

> Dans une optique constructiviste, le risque ne caractérise plus un élément du monde extérieur — le danger —, mais il est conçu comme un artefact associé aux peurs collectives, résultat de l'interaction entre le contexte socioculturel et, dans une certaine mesure, le monde extérieur. Ce que met explicitement en lumière la conception constructiviste, c'est l'influence socioculturelle sur la manière dont le sujet conçoit les risques. (Kermisch, 2012, p. 6)

L'évaluation des risques dans ce second paradigme s'appuie moins sur la position d'un expert, mais davantage sur des processus délibératifs qui permettent de faire émerger la pluralité des points de vue sur ce qui constitue un risque, en tenant compte des différentes parties prenantes d'une situation ou d'un projet.

Toujours selon Kermisch, ces deux conceptions du risque ne sont pas opposées, mais complémentaires. Elle propose ainsi d'adopter une position sur le risque qui relie les deux :

> Opter pour une définition multidimensionnelle du risque présente l'avantage d'offrir un outil conceptuel riche, dans la mesure où la composante quantitative chiffre le potentiel de dommages, alors que la composante constructiviste rend compte du

> risque compris comme représentation des inquiétudes individuelles et collectives, lesquelles figurent au programme d'une gestion des risques qui rende compte du pluralisme social et qui soit acceptable sur le plan de l'éthique. (2012, p. 6)

Cette définition multidimensionnelle du risque n'est pas sans avoir d'impact sur les processus d'évaluation eux-mêmes. Si, traditionnellement, la partie quantitative s'appuie davantage sur l'expertise et la connaissance du domaine d'affaires de l'objet évalué, la prise en charge du volet quantitatif nécessite d'ajouter une étape « destinée à mettre en lumière les enjeux qualitatifs en présence, qu'ils soient éthiques, politiques ou socioculturels » (2012, p. 10). Cette évaluation peut, comme le dit Kermisch, s'effectuer dans le cadre d'une démarche participative. Je m'avance un peu dans mon propos, mais cette manière de concevoir le risque paraît tout à fait pertinente en ce qui concerne les risques et les préjudices portés à la vie privée, car leur matérialisation repose, dans les faits, sur la perception qu'en ont les personnes. J'aborderai cette question davantage dans les second et troisième chapitres de ce mémoire.

Concernant l'ÉFVP et les processus d'évaluation des risques et des préjudices en matière de protection de la vie privée, il s'agira de déterminer comment ces différents paramètres seront opérationnalisés, par exemple : quelle sera la nature des risques évalués? Comment interpréter la notion de « probabilité »? Comment établir les seuils d'intensité des préjudices? Quels seront les sujets des risques évalués? Les risques encourus par l'organisation, par les individus concernés, par des groupes vulnérables et marginalisés ou par la société dans sa globalité? Est-ce que les parties directement concernées seront impliquées dans le processus d'évaluation?

1.4.2 Le domaine d'application et la détermination des risques à évaluer

Dans la norme ISO 31000 – *lignes directrices pour le management du risque* (2018) (document qui vise les évaluations de risque de façon générale), l'ISO souligne l'importance pour une organisation de définir quel est le *domaine d'application* (ou le *périmètre d'application*) d'un processus d'évaluation de risques. Cette notion est importante pour les activités de management du risque. Il s'agit de définir la portée du processus d'évaluation et

de déterminer l'étendue et la nature des risques envisagés dans l'exercice. Il s'agit « d'être précis quant au domaine d'application considéré, aux objectifs pertinents à prendre en compte et à leur alignement sur les objectifs de l'organisme » (2018, s. p.). La norme ISO énonce d'autres critères qui permettent de définir le domaine d'application d'une activité de gestion de risque. J'en retiens deux qui m'apparaissent plus importants à l'égard de mon sujet, soit « les objectifs » et « les inclusions et exclusions spécifiques ». Les autres critères ont leur importance, mais sont davantage d'ordre opérationnel. Il s'agit, notamment, des outils d'appréciation du risque utilisés (formulaires, questionnaires, rencontres de travail, etc.), des ressources nécessaires pour tenir l'activité (ressources humaines, financières, matérielles, etc.), la documentation rattachée à l'exercice (rapports, formulaires, etc.) et les relations entretenues entre le processus d'évaluation des risques et des préjudices avec les autres projets, processus et activités d'une organisation (la place qu'occupe un tel processus à l'intérieur d'une fonction plus large de surveillance des activités d'une organisation, par exemple avec les activités de vérification interne).

Il semble couler de source que l'objectif principal de l'ÉFVP devrait être la protection de la vie privée. L'échafaudage législatif mis en place par le projet de loi no 64 (désormais, la Loi 25) visait clairement à améliorer le niveau de protection accordée à la vie privée, ce qui démontrait le souci éthique accordée à cette dimension de l'existence humaine dans la société québécoise. Ainsi, l'ISO, le CPVPC et la CAI font explicitement mention des impacts potentiels sur la vie privée des personnes visées par les processus ou les systèmes qui sont évalués lors de la réalisation de l'ÉFVP. L'Union européenne fait référence plus largement aux droits et libertés des personnes, ce qui inclut généralement le droit à la vie privée. Seule la définition du *Department of Justice* américain ne semble pas faire référence à la protection de la vie privée des individus, leur PIA visant à démontrer que des mesures de sécurité de l'information ont été déployées à toutes les étapes du traitement de l'information. La confusion entre les termes de « Privacy » anglais et de « protection de la vie privée » peut sans doute concourir à expliquer cette impression que le PIA ne vise que la mise en place de mécanisme de sécurisation de l'information. Les définitions rapportées à la section 1.3 identifient également certains objectifs secondaires, par exemple : s'assurer de la conformité

et du respect des lois ou démontrer la prise en charge de la sécurité des renseignements personnels. Ces deux objectifs concourent sans aucun doute à la protection de la vie privée, mais l'objectif principal — protéger la vie privée — n'est pas entièrement couvert ni par le premier objectif secondaire ni par le second.

Ainsi, il faut bien déterminer en amont quel sera le « terrain de jeu » du processus d'évaluation au risque de ne pas atteindre l'objectif premier. En déterminant son domaine d'application, l'organisation établit clairement quels sont les éléments visés par l'évaluation, et quels sont ceux qui ne seront pas considérés dans la gestion des risques. Le domaine d'application d'un évaluateur qui se donne pour objectif d'être simplement conforme aux lois en vigueur mènera celle-ci à considérer principalement quels sont *ses* risques juridiques. Elle aura également à considérer minimalement les risques posés par la sécurité de l'information qu'elle détient, non parce que c'est important, mais parce qu'elle y est obligée par la loi, et être conforme requiert qu'elle s'y attarde. L'évaluateur qui, quant à lui, cherche uniquement à s'assurer que les mesures de sécurité de l'information et de cybersécurité sont suffisantes ne se penchera pas nécessairement aux enjeux de protection des renseignements personnels. Dans les deux cas, les considérations en lien plus largement avec la protection de la vie privée, que j'aborde plus en détail au chapitre 2, pourraient ne pas être considérées.

Cette précision peut sembler évidente ou superfétatoire, mais la question se pose consciemment ou non lorsqu'un processus de gestion des risques est mis sur pied. La détermination du domaine d'application propre à la protection de la vie privée devrait permettre de déterminer la nature des événements qui seront pris en compte dans l'évaluation. Mais le fait de déterminer le « terrain de jeu » veut nécessairement dire que certains événements en seront exclus : il y aura inévitablement des « externalités » qui ne seront pas prises en compte dans les processus. En excluant d'entrée de jeu certains pans de la protection de la vie privée de processus d'évaluation de la gestion de risque, les exclusions deviennent autant d'effets externes potentiels qui ne seront pas appréciés par l'organisation.

Ainsi, les critères menant à l'inclusion ou à l'exclusion de risques peuvent concerner : la nature des événements (financiers, juridiques, économiques, de sécurité de l'information,

les dangers à la santé, etc.); un seuil minimal de probabilité ou de gravité des impacts en dessous duquel les risques ne sont tout simplement pas considérés; et, finalement, l'entité qui est sujette aux préjudices advenant la matérialisation des risques évalués. Ce dernier critère requiert davantage d'explicitation. La détermination du sujet du risque influence directement l'évaluation du risque. Ainsi, une organisation qui s'intéresse aux seuls risques (qu'ils soient juridiques, financiers, stratégiques, etc.) *qu'elle encoure elle-même* réalisera un processus d'évaluation des risques et des préjudices bien différent de celui qu'elle réalisera si elle s'intéresse plutôt aux risques *qu'elle fait encourir à* sa clientèle, à ses partenaires d'affaires, à ses investisseurs, etc. Dans le premier cas, elle s'intéressera aux risques d'encourir des plaintes, des risques de poursuites juridiques, des enjeux commerciaux, stratégiques ou financiers, ou des risques de dommages à sa réputation, etc. Certes, elle évaluera les enjeux de protection de renseignements personnels, mais toujours dans l'objectif d'être conforme aux lois et non dans celui de protéger la vie privée des personnes visées par l'activité qu'elle évalue. Ce faisant, elle évaluera bien sûr des risques à la protection de la vie privée, mais de façon accidentelle. En mettant l'accent sur l'organisation et non sur les personnes, l'exercice de gestion de risque conserve un angle mort important : la perception de l'individu sur ce qui constitue une atteinte à la vie privée[20].

L'individu devrait donc normalement se trouver au cœur des préoccupations lors de l'évaluation des risques et des préjudices à la vie privée. C'est d'ailleurs pourquoi la plupart des organismes de surveillance (de ce nombre, le CPVPC, la CAI et l'Union européenne) mettent la protection des personnes concernées au cœur des exercices d'ÉFVP. Mais même ainsi, la question suivante reste entière : s'il ne s'agit pas d'évaluer uniquement les risques en matière de protection des renseignements personnels ou en matière de sécurité de l'information ou de cybersécurité, quels sont les risques qu'il convient d'identifier, de mesurer et d'éliminer ou de mitiger en matière de protection de la vie privée?

[20] Je reviens sur ce point dans la section 2.3.2 alors que j'aborde les travaux de la théoricienne Helen Nissenbaum sur la protection de la vie privée informationnelle en tant que norme liée à l'intégrité contextuelle.

1.4.3 Définir le risque et le préjudice porté à la protection de la vie privée

Les différents guides de réalisation d'ÉFVP consultés dans le cadre de cette recherche proposent tous des définitions de *risque en matière de protection de la vie privée.* De fait, bien que les définitions rapportées dans la section précédente se rejoignent dans les grandes lignes, il ne semble pas exister de compréhension commune de ce qui constitue un risque en matière de protection de la vie privée. Dans un document produit en 2006 pour le compte du SRIDAIL et destiné aux organismes publics, le risque (identifié ici comme étant un scénario de risque) est ainsi défini par Dionne :

> Un scénario est un événement, ayant une origine et une cause, qui entraîne des répercussions négatives sur la protection des renseignements personnels. À titre d'exemple, citons la divulgation, par un membre du personnel d'un ministère ou d'un organisme public, de renseignements personnels à des personnes non autorisées. (2006, p. 10)

La lecture de cette définition montre que les risques évalués sont ici limités à ceux liés à des enjeux de protection des renseignements personnels, donc à des enjeux d'abord et avant tout juridiques. Il s'agit davantage d'un audit sur les pratiques organisationnelles en matière de protection des renseignements personnels et, du propre aveu des auteurs, « [b]ien que les scénarios de risques proposés dans ce document recouvrent le cycle de vie d'un renseignement personnel ainsi que les obligations légales s'y rapportant, d'autres risques liés à la protection de ce type de renseignement peuvent ne pas avoir été pris en considération » (Dionne, 2006, p. 6).

La CAI pour sa part définit le risque à la vie privée comme « un événement qui causerait une perte ou un préjudice à une personne au niveau du respect de son intimité ou de sa vie personnelle. » Elle précise également que

> la perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (exemple : en cas de dommage à la réputation), où être vécus de l'intérieur par les personnes concernées (exemple : sentiment d'intrusion). (2021, p. 16)

Quant à lui, le Commissariat à la protection de la vie privée du Canada (CPVPC) stipule que l'

> ÉFVP met l'accent sur les atteintes à la vie privée, plus précisément sur le risque d'atteinte à la vie privée d'individus et aux droits que leur confère la LPRP. Par conséquent, votre analyse de l'incidence des risques devrait prendre en compte le type de préjudice qu'une personne pourrait subir si le risque se matérialisait. Par exemple, la réputation, la situation financière ou le bien-être émotionnel de la personne seraient-ils menacés? (2011, s. p.)

Finalement, l'Énoncé de politique des trois conseils (EPTC2) encadrant la recherche avec les humains au Canada présente le risque en matière de la vie privée comme étant les « [p]réjudices potentiels que peuvent subir les participants, ou les groupes auxquels ils appartiennent, à cause de la collecte, de l'utilisation et de la divulgation de renseignements personnels dans le cadre d'une recherche » (Gouvernement du Canada, 2018, p. 227).

Pour ces trois dernières organisations, le domaine d'application de l'évaluation des risques et des préjudices doit déborder de la seule dimension juridique, car la notion de risques à la protection de la vie privée s'étend à des éléments qui ne relèvent pas strictement de la conformité aux lois de protection des renseignements personnels pour viser également la problématique plus grande de la protection de la vie privée. De plus, ces organisations détournent l'attention des organisations qui produisent l'évaluation vers les personnes concernées par la collecte, l'utilisation ou la communication de renseignements personnels. Elles étendent ainsi la notion de risques à la protection de la vie privée à des éléments qui ne relèvent pas strictement de la conformité aux lois de protection des renseignements personnels pour viser également la problématique plus grande de la protection de la vie privée. À quoi pourrait ressembler une liste de scénarios de ces risques?

Solove s'est penché sur cette question dans son ouvrage *Understanding privacy*[21]. Dans ce livre, il propose d'aborder la question de la vie privée en s'inspirant à la fois de la philosophie wittgensteinienne et du pragmatisme de John Dewey. S'appuyant sur la théorie

[21] Ce livre reprend des éléments d'abord explorés par l'auteur dans des articles antérieurs (Solove, 2002, 2006)

des jeux de langage de Wittgenstein, Solove abandonne la recherche d'un dénominateur commun propre à toutes les conceptions de la notion de « protection de la vie privée ». Il privilégie ainsi une compréhension pluraliste de celle-ci : « "Privacy" is an umbrella term that refers to a wide and disparate group of related things. » (2008, p. 45) L'emprunt à Wittgenstein lui permet de faire l'économie de la recherche d'un point théorique focal, un centre conceptuel à partir duquel toutes les acceptions du terme « protection de la vie privée » découleraient. Au lieu de cette recherche de l'unité, il cherche à rassembler sous forme de taxonomie ces éléments qui partagent un « air de famille », selon la formule wittgensteinienne (2008, p. 43; Wittgenstein et Rigal, 2014, p. 64-65)[22]. De Dewey, Solove retient une méthodologie fondée sur une approche empirique, contextuelle et « bottom-up » plutôt qu'une approche idéaliste et « top down » : « Pragmatism emphasizes that we begin philosophical inquiry with the problems we need to solve. » De ce fait :

> A theory of privacy should focus on the problems that create a desire for privacy. Privacy concerns and protection does not exist for their own sake; they exist because they have been provoked by particular problems. Privacy protection are responses to problems caused by friction in society. (2008, p. 75-76)

Au lieu de chercher de manière déductive les différentes catégories de « protection de la vie privée », il s'alimente plutôt des situations concrètes qui ont engendré un besoin de protection de vie privée. Celle-ci lui permet d'identifier quels sont les éléments qui partagent l'air de famille particulier de la « protection de la vie privée ». Pour établir sa taxonomie, il parcourt la jurisprudence et les lois de protection de la vie privée afin d'identifier quels ont été les problèmes que les juristes et législateurs ont cherché à résoudre. Ainsi, pour Solove, le droit à la vie privée est constitué d'un ensemble de mécanismes de protection mis en place pour répondre à des activités qui ont été perçues avec le temps comme posant potentiellement des préjudices à la vie privée. En procédant ainsi, Solove échafaude une taxonomie de la vie privée qui demeure ouverte à la contingence et au caractère évolutif du concept de « vie

[22] Je souligne que la nature pluraliste de la protection de la vie privée est abordée de nouveau dans la section 2.3.1.

privée » (sa « variability »), mais qui permet tout de même d'atteindre un niveau suffisant de généralité et de flexibilité pour pouvoir être utilisée dans différents contextes.

C'est ainsi qu'il propose une taxonomie des activités qui peuvent engendrer potentiellement une atteinte à la protection de la vie privée. Il identifie dix-huit activités qui sont susceptibles d'être perçues comme un problème posé à la vie privée. Il les regroupe au sein de quatre grandes familles d'activités :

- les activités de collecte d'information, soit la surveillance (sous toutes ses formes) et les interrogations (en incluant les fouilles physiques);

- les activités de traitement de l'information, soit l'agrégation d'information (le croisement de plusieurs sources), l'identification (lier une information à l'identité d'une personne), l'insécurité informationnelle (le fait de ne pas protéger suffisamment de l'information détenue sur autrui), l'utilisation secondaire de l'information (utilisation pour laquelle la personne concernée n'a pas été informée), et le fait de maintenir une personne concernée dans l'ignorance (« exclusion ») quant au fait que de l'information la concernant est détenue ou utilisée;

- les activités de dissémination d'information[23], soit la violation de la confidentialité, la divulgation intentionnelle d'information, l'exposition du corps (par exemple, par une photographie), le fait d'accroître l'accessibilité de l'information, l'usage d'information pour faire chanter, l'usurpation d'identité, la diffusion de fausses informations sur une personne, ainsi que les activités qui impliquent une immixtion dans la vie privée, soit l'intrusion dans l'intimité d'une personne ou l'ingérence dans un processus décisionnel personnel.

[23] Au Québec, le terme « information dissemination » serait possiblement traduit par « communication de l'information ».

Solove précise que la réalisation de l'une de ces activités n'entraîne pas nécessairement d'atteintes à la vie privée ou des préjudices. Par exemple, ce ne sont pas toutes les activités de surveillance qui seront perçues comme étant préjudiciables : la surveillance des frontières pour gérer les entrées illégales n'entraîne pas de préjudices pour l'ensemble des voyageurs qui les traversent. Du moins, même si la surveillance par un état des allées et venues sur son territoire est une atteinte à la vie privée dans l'absolu, peu de voyageurs perçoivent cette intrusion comme étant un préjudice (sauf peut-être ceux qui s'apprêtent à enfreindre une loi comme le fait d'importer des substances illégales). L'utilisation secondaire de renseignements médicaux pour la recherche de nouveaux médicaments peut au contraire s'avérer bénéfique, à la fois pour la société et pour la personne concernée (advenant qu'elle-même devienne consommatrice dudit médicament).

Nous trouvons dans cette taxonomie les éléments propres à établir un bassin de scénarios de risques à évaluer par une organisation dans le cadre d'une ÉFVP. Les activités qui y sont décrites sont des *événements* qui concernent la vie privée des personnes (les *sujets*). Ces événements ont le potentiel (la *probabilité*) de se matérialiser et de causer une atteinte ou un préjudice (un *impact*) dont la gravité pourrait varier. La question de la *nature* des préjudices reste cependant ouverte.

Solove a établi une autre taxonomie, cette fois-ci en partenariat avec Danielle Keats Citron (Solove et Citron, 2021). Cette seconde taxonomie identifie les atteintes et les préjudices causés à la vie privée. Ils ont dénombré sept catégories de torts et de préjudices pouvant résulter d'une activité posant un problème à la vie privée, soit : 1) les préjudices physiques; 2) les préjudices économiques; 3) les préjudices liés à la réputation; 4) les préjudices liés à la discrimination; 5) les préjudices portés aux relations d'une personne; 6) les préjudices portés à l'autonomie d'une personne; et 7) les préjudices psychologiques. La catégorie des préjudices portés à l'autonomie d'une personne regroupe six sous-types de préjudices, soit : la coercition effectuée sur le sujet des renseignements personnels; la manipulation de celui-ci; un choix mal-informé ou de la non-connaissance d'un droit en raison d'information imprécise ou manquante; la contrariété ressentie par le non-respect des

attentes raisonnables en matière de vie privée (« thwarted expectations harms »); les préjudices liés à la perte du contrôle sur les renseignements personnels; et, finalement, l'effet dissuasif sur les personnes qui les fait hésiter à exercer leurs droits ou leurs libertés (le « chilling effect »). Quant à elle, la catégorie des préjudices psychologiques renferme la détresse émotionnelle engendrée par une atteinte à la vie privée ainsi que la nuisance et le simple dérangement.

Kröger, Micelli et Müller ont également proposé une taxonomie des préjudices liés à des atteintes à la vie privée, mais spécifiquement pour les situations en lien avec l'utilisation des données numériques. Ils ont recensé onze situations liées spécifiquement à l'usage malicieux des données (Kröger *et al.*, 2021). Ces différentes situations où les données sont utilisées pour causer du tort sont : 1) l'utilisation pour des fins de gratification personnelle (par exemple, le voyeurisme ou la moquerie); 2) l'obtention d'un avantage coercitif (par exemple, pour faire chanter quelqu'un ou pour l'inciter à modifier un comportement en exploitant ses faiblesses); 3) le contrôle de la conformité (par exemple, la surveillance des individus ou le fait de mesurer des performances, etc.) 4) le discrédit (par exemple, causer un tort à la réputation); 5) les processus d'évaluation et de discrimination (par exemple, déduire de nouvelles informations à partir de données existantes pour déterminer des caractéristiques ou classifier les individus); 6) l'identification de points faibles en vue de causer du tort dans la réalité (par exemple, cerner les vulnérabilités physiques, psychologiques, financières ou sociales d'un individu ou d'un groupe d'individus); 7) la persuasion personnalisée (par exemple, le ciblage publicitaire ou les attaques d'ingénierie sociale); 8) la sollicitation directe de la personne concernée (par exemple, les tentatives de fraude en ligne); 9) la localisation physique d'une personne (par exemple, en vue de perpétrer un acte de vengeance ou pour harceler); 10) la saisie d'autres actifs informationnels (par exemple, l'accès illégitime à un compte en banque le vol d'identité); et, finalement, 11) l'utilisation stratégique des données (par exemple, l'utilisation des données et des systèmes d'intelligence artificielle pour faire de la police prédictive).

La combinaison des taxonomies de Solove et de Keats Citron ou la taxonomie de Kröger, Micelli et Müller nous fournissent des ébauches de liste de scénarios de risques intéressants pour entamer un exercice d'évaluation des risques et des préjudices à la protection de la vie privée. J'aimerais toutefois apporter un point sur la nature des risques et des préjudices portés à la vie privée qui, à la lumière des taxonomies de Solove et de Keats Citron, prennent les allures de risques éthiques. L'Énoncé de politique des trois conseils (EPTC) sur l'éthique de la recherche avec des êtres humains définit le risque éthique de cette manière :

> Comme la recherche est un pas vers l'inconnu, elle risque de causer des préjudices aux participants et à d'autres personnes. On entend par préjudice tout effet négatif sur le bien-être des participants. Le préjudice peut être de nature sociale, comportementale, psychologique, physique ou économique. Le risque est fonction de l'ampleur ou de la gravité du préjudice et de la probabilité que les participants ou des tiers le subissent (comme il est indiqué ci-après). L'analyse convenable d'un projet de recherche, sur le plan de l'éthique, devrait tenir compte des risques prévisibles et des moyens disponibles pour les supprimer ou les atténuer. (Gouvernement du Canada, 2018, p. 22)

Solove et Keats Citron tissent eux aussi des liens entre les risques et les préjudices portés à la vie privée et les dimensions physique, économique, réputationnelle, relationnelle et psychologique des personnes concernées et soulignent qu'ils peuvent concerner des atteintes à leur autonomie ou se solder en effets discriminatoires à leur endroit. Johnston étend également la notion de préjudices causés par une atteinte à la vie privée à des sphères qui débordent largement les seuls risques portés aux renseignements personnels :

> Privacy harms exist across a spectrum, and include: tangible or 'material' harms at one end (such as physical harm or threats of violence, stalking and harassment, identity theft, financial loss and psychological damage), intangible or 'moral' harms in the middle (such as reputational damage, "creepy inferences," humiliation, embarrassment or anxiety, loss of autonomy, discrimination and social exclusion), and shared or 'social' harms at the other end (such as the threats to democracy, chilling effect on free speech, loss of trust and social cohesion posed by a 'surveillance society', and by manipulation and amplification of political messaging on social media). (Johnston, 2020, p. 8)

Or, la définition de l'EPTC fait référence aussi à ces dimensions pour les risques éthiques. Ainsi conceptualisée, l'évaluation des risques et des préjudices portés à la vie privée se confondrait avec l'évaluation plus générale des risques éthiques. Évaluer un projet dans l'objectif de maximiser les bénéfices encourus et de minimiser ou d'éliminer les risques portés à la vie privée reviendrait ainsi à évaluer ce projet d'un point de vue éthique.

1.5 *CONCLUSION*

En abordant la question de la nature des risques en matière de la protection de la vie privée, j'ai tenté de montrer qu'il n'est pas simple de déterminer le domaine d'application qui devrait être celui de l'ÉFVP. L'exercice en lui-même variera grandement en fonction de différents paramètres. D'abord, les risques évalués vont varier en fonction des obligations légales et réglementaires de la législation dans laquelle l'exercice est tenu. Ils varieront également en fonction de la portée et de l'envergure du projet ou de l'initiative soumis à l'évaluation, puis des objectifs (financiers, stratégiques, juridiques, éthiques, etc.) de l'organisation qui le tient. Finalement, on peut penser que le champ d'expertise et les intérêts des personnes qui effectuent la mise en œuvre de cette évaluation de risques teinteront la nature des risques qui seront considérés : le juriste ou le spécialiste en protection des renseignements personnels s'attardera davantage aux risques juridiques; l'administrateur considérera les enjeux stratégiques ou financiers liés à l'utilisation des renseignements personnels; les informaticiens et autres technologues s'attarderont plutôt aux risques en matière de sécurité de l'information[24] ou aux cybermenaces qui pèsent sur les systèmes

[24] Il est généralement question d'évaluation des risques en *sécurité de l'information* dans les grands projets informatiques. La sécurité de l'information est entendue par les spécialistes comme l'« [e]nsemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire » (OQLF, 2021b). Les trois dimensions mentionnées par l'OQLF (confidentialité, intégrité et disponibilité) sont généralement présentes dans les référentiels ou les gabarits d'évaluation de risques, mais le nombre de dimensions évaluées peut changer selon la méthodologie appliquée. Par exemple, le Secrétariat du Conseil du trésor du Québec ajoute également des risques liés à l'irrévocabilité et à l'authentification.

informatiques eux-mêmes[25]; etc. La plupart de ces dimensions n'entrent pas en contradiction entre elles : qu'ils soient juridiques, stratégiques ou liés à la sécurité de l'information, la mitigation ou l'élimination des risques concourent sans aucun doute généralement à améliorer la protection de la vie privée des personnes concernées. Les enjeux couverts par la protection des renseignements personnels et ceux couverts par les mesures de sécurité de l'information et de cybersécurité sont distincts, mais ils sont complémentaires et interreliés. (Roussel et Bistodeau, 2009, p. 5)

Il faut se rapporter à la notion de domaine d'application pour déterminer quels seront les risques considérés dans l'exercice qu'est la réalisation d'une ÉFVP. Rappelons-nous que la notion d'objectif est centrale pour établir le domaine d'application. Est-ce que le processus d'évaluation vise à établir la conformité légale du projet à l'étude? Vise-t-il plutôt à garantir la sécurité des renseignements personnels qui sont détenus par l'organisation qui procédera à la mise en œuvre du projet? Vise-t-on à protéger les intérêts propres à l'organisation ou ceux des personnes concernées par le projet? Si l'on en croit ce que les différents documents consultés nous ont signalé, l'objectif de l'ÉFVP devrait être, en réalité, la protection de la vie privée des personnes concernées par le projet évalué. Ainsi, la nature des risques évalués devrait, en théorie, découler directement de l'objet qui doit être protégé. Or, cet objet — la « protection de la vie privée » — est difficile à cerner. Le prochain chapitre vise à mettre en lumière cette complexité et à voir en quoi elle rend plus difficile le fait de poser des paramètres à la réalisation d'une ÉFVP.

[25] Nous pouvons penser ici aux risques liés à la cybersécurité, comme le risque d'intrusion dans les systèmes par un tiers en raison d'une défaillance logiciel.

CHAPITRE 2
QU'EST-CE QUE « PROTÉGER LA VIE PRIVÉE »?

2.1 *INTRODUCTION*

De manière générale, l'évaluation des risques et des préjudices à la protection de la vie privée constitue la moitié de ce que représente une évaluation des facteurs relatifs à la vie privée (ÉFVP), l'autre moitié étant la vérification de la conformité légale du projet à l'étude. Au Québec, la vérification de la conformité légale implique aussi d'établir des mécanismes en matière de sécurité de l'information et de cybersécurité qui sont suffisants pour garantir une protection raisonnable des renseignements personnels. Les aspects juridiques et technologiques de cet exercice ne sont pas moins complexes l'un et l'autre. Ils requièrent un niveau de connaissance élevé et spécialisé, soit une connaissance des lois en vigueur et des principes de sécurité de l'information, et une maîtrise des processus d'évaluation des risques et des préjudices. Pour ce deuxième élément, il est essentiel d'établir la nature de l'objet auquel ces risques font référence pour s'assurer d'atteindre l'objectif de l'exercice. En effet, de manière à bien comprendre ce que pourrait être un risque porté à la vie privée, encore faut-il avoir une certaine idée de ce qui doit être protégé contre ces risques, c'est-à-dire la « vie privée ». C'est la question à laquelle je désire m'attarder dans ce second chapitre.

La réponse peut sembler très simple : nous avons tous une connaissance intuitive et immédiate de notre propre « vie privée ». Spontanément, nous pouvons rattacher cette idée à la dimension « biographique » de notre existence ou à notre intimité : « c'est de ma vie » dont il est question lorsqu'il est question de « ma vie privée », de mon histoire, de ma constitution physique, de mes relations interpersonnelles, de mes finances, etc. Cependant, la personne qui s'attarde quelque peu à définir ce qui est entendu par la notion théorique de « vie privée » (comme il est entendu dans les expressions « protection de la vie privée » ou « droit à la vie privée ») constate assez rapidement qu'elle se trouve face à une notion complexe, multiple et, surtout, conflictuelle. Comme d'autres l'ont fait, Richards invoque

l'anecdote suivante pour illustrer le paradoxe entre l'immédiateté sensible du concept de « protection de la vie privée » et la complexité théorique dont il fait l'objet :

> If you want to get really depressed about the difficulties of definition, consider obscenity law, which to this day remains haunted by Justice Potter Stewart's frustration at the U.S. Supreme Court's inability to define obscene movies separately from nonobscene ones with his famous declaration, "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But *I know it when I see it*, and the motion picture involved in this case is not that." (Richards, 2022, p. 21)

Le parallèle qui est fait ici entre la protection de la vie privée et le matériel pornographique peut sembler surprenant. Néanmoins, à l'instar du juge Stewart qui, face à ce matériel « obscène », n'a cure du débat théorique pour émettre son jugement, nous faisons souvent l'économie d'une réflexion approfondie sur la question.

Dans un rapport récent d'analyse concernant l'Internet des objets, la Commission de l'éthique en science et en technologie du Québec (CEST) a contourné le problème de la définition de la protection de la vie privée de façon plus élégante. En s'appuyant sur la notion de *consensus par recoupement* de John Rawls, la CEST décide de ne s'attarder qu'aux situations qui font consensus en tant qu'« atteinte » ou « problème » portés à la vie privée, sans porter d'égards aux enjeux et divergences théoriques que la définition soulève. Elle est d'avis que « [c]ertaines situations claires illustrent des infractions au droit à la vie privée, quelle que soit la justification en faveur du droit à la vie privée » (CEST, 2020, p. 13). Malgré les divergences théoriques parfois profondes qui peuvent exister entre tel et tel auteur ou entre telle ou telle conception de la protection de la vie privée, il est toujours possible d'atteindre un certain consensus sur ce qui constitue ou non une atteinte à la vie privée. Des cas de figure comme le voyeurisme, la fouille abusive ou la consultation de courriers confidentiels par un tiers non autorisé font partie de ces situations dont le statut d'« atteinte à la vie privée » est généralement admis. Elle laisse de ce fait aux théoriciens la tâche de s'attarder aux situations limites et de « trancher les débats substantiels entourant la notion de vie privée et sa justification » (CEST, 2020, p. 13).

Pourquoi dès lors chercher à obtenir une définition de ce qu'est la vie privée si nous pouvons faire fi des débats théoriques? Parce que je pense que cette perception intuitive et immédiate de la protection de la vie privée n'épuise pas tous les sens et les éléments qui ont été accolés à ce concept au fil du temps. En outre, et j'y reviens dans le troisième chapitre de mon mémoire, certaines caractéristiques de l'objet « protection de la vie privée » peuvent moduler de façon importante ce qui peut être visé par un processus d'évaluation des risques et des préjudices en matière de vie privée.

Ce chapitre vise donc d'abord à mettre en lumière les débats théoriques qui entourent la question de la nature de la vie privée et de sa protection. Dans les deux prochaines sections, je m'attarderai à recenser certaines réponses qui ont été données à la question « *qu'est-ce que "protéger la vie privée"? »* La section 2.2 dresse un portrait succinct des principales théories de la protection de la vie privée qui ont été élaborées au XXe siècle. L'objectif plus spécifique est de montrer que ces réponses quant à la nature de la protection de la vie privée sont en fait très peu consensuelles. Cette absence de consensus peut s'expliquer du fait que la protection de la vie privée est un concept multidimensionnel (section 2.3), qui est fortement lié au contexte duquel il émerge (section 2.3.2) et qui est potentiellement litigieux dans son essence même (section 2.3.3). Fort de ces constats, je propose par la suite d'adopter la position du professeur de droit américain Neil Richards en préférant m'attarder à la *valeur instrumentale* que peut revêtir la protection de la vie privée au détriment de la recherche d'une hypothétique essence qui lui accorderait un statut privilégié dans l'ordre des droits et libertés de la personne.

2.2 *LES ÉCUEILS DES APPROCHES DESCRIPTIVES DE LA PROTECTION DE LA VIE PRIVÉE*

2.2.1 Caractériser les conceptions théoriques de la protection de la vie privée

Le concept de « vie privée » a fait l'objet de nombreux travaux de la part de théoriciens, dans des domaines aussi variés que la philosophie, le droit, l'histoire, l'anthropologie, la sociologie, la psychologie, etc. L'histoire du concept montre en effet qu'il jouit d'une très

longue vie. Les tentatives de définir quelque chose comme la « vie privée » remonteraient au moins à l'Antiquité, alors qu'Aristote proposait de faire la distinction entre les choses qui relèvent de la vie domestique et celles qui relèvent de la vie publique (DeCew, 2018). Les recherches historiques montrent également que les individus se préoccupaient de quelque chose comme leur « vie privée » depuis au moins aussi longtemps (Duby et Ariès, 1999). L'idée et la formalisation d'un droit spécifique à la vie privée sont cependant beaucoup plus récentes.

On situe généralement en 1890 l'émergence du débat contemporain sur la question de la « protection de la vie privée » et de l'existence d'un « droit à la protection de la vie privée » avec la parution de l'article *The Right to Privacy* écrit par les juges américains Louis D. Brandeis et Samuel D. Warren (1890). Leur réflexion s'inscrivait à l'époque dans un contexte marqué par l'émergence de la presse écrite. Face à l'apparition des appareils photographiques, qui menaçaient selon eux « l'enceinte sacrée de la vie privée et domestique » par la « diffusion non-autorisée de portraits » et le risque que « ce qui se dit dans les placards soit répété sur tous les toits », ces deux juges défendaient l'idée d'un droit à être *laissé seul* (idée mieux rendue en anglais par le terme de « right to be left alone »). Ils considéraient important d'établir une protection légale pour protéger l'intimité des personnes, de manière à prévenir l'invasion de leur espace privé. Dans le sillage de la parution de cet article dans la *Harvard Law Review*, une multitude de pages ont été écrites par les juristes et les philosophes. Malgré ce foisonnement de documentation, la confusion entourant les différentes conceptions de la « vie privée », de la « protection de la vie privée » et du « droit à la vie privée » persiste à ce jour. Comme le souligne DeCew à juste titre, « [t]he term "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term » (DeCew, 2018). Certains auteurs ont voulu faire le ménage dans ces concepts et ont proposé différentes façons de classifier et de caractériser les réponses données à la question portant sur la nature de la vie privée.

Par rapport au corpus imposant qui a été produit sur le sujet, Kevin Macnish écrit (les italiques sont de moi) :

> In summary, the last 130 years, and particularly the last 50 years, have seen a large amount of activity regarding privacy. Legal decisions have frequently been occasioned by developments in technology that have given the state and other actors (such as companies) access to hitherto private information, and have typically responded by restricting this access. Philosophical debate has tended to focus on the *meaning*, *extent*, and *value of privacy*. (Macnish, 2019, p. 5)

Du point de vue philosophique, Macnish nous informe que le sujet est traversé par trois questions distinctes. La première question pourrait être reformulée ainsi : *qu'est-ce que la vie privée?* Il s'agirait ici de définir ontologiquement la nature de ce qui est visé par le droit à la vie privée ou par les mécanismes de protection qui sont mis en place pour ce faire. La seconde pourrait être reformulée en ces mots : *quels sont les phénomènes qui sont visés par la protection de la vie privée?* Il s'agirait ici de cerner son champ d'application et de voir à quels objets elle s'applique. La troisième question, la plus importante pour la question proprement éthique, pourrait être reformulée ainsi : *pourquoi devons-nous protéger la vie privée?* Cette question cherche à établir la finalité visée par cette protection et déterminer quelles sont les valeurs poursuivies par la mise en place d'une protection de la vie privée. Ces trois questions sont distinctes, mais l'objet qu'elles cherchent à décrire demeure le même, c'est-à-dire la vie privée en elle-même. L'auteur qui voudrait s'attaquer à la recension des différentes réponses proposées par les théoriciens tout au long des 130 dernières années pourrait le faire à partir de ces trois critères. Sans reprendre intégralement ce découpage pour traiter ces questions, j'essaie tout de même d'esquisser des réponses tout au long de ce second chapitre, à la hauteur de ce que peut être un mémoire de maîtrise. La première question est traitée en filigrane tout au long du chapitre. Alors que la section 2.3.1 portant sur les approches taxonomiques et typologiques de la vie privée répond un peu plus spécifiquement à la seconde question, la section 2.4 offre certaines pistes de réponses à la troisième.

Benyekhlef et Déziel distinguent également les conceptions théoriques selon qu'elles sont uniquement *descriptives* (elles cherchent à décrire *l'état actuel* de la protection de la vie

privée) ou qu'elles ont une portée *normative* (elles cherchent à définir ce que la protection de la vie privée *devrait* être). Ces deux auteurs sont issus du domaine du droit et ils s'attardent, de ce fait, plutôt aux théories purement juridiques du droit à la protection de la vie privée : « On qualifie de descriptives les théories qui entendent à présenter de manière objective ce qu'est le droit. Ce sont des théories qui, en d'autres mots, tentent de dresser le portrait du droit et d'en présenter les principales caractéristiques sans poser de jugement de valeur sur celles-ci. » (Benyekhlef et Déziel, 2018, p. 15) Ils poursuivent ainsi au sujet des théories normatives :

> Les théories normatives entendent plutôt prendre position sur ce que devrait être le droit. En ce sens, l'élaboration d'une théorie normative exige un travail préliminaire de description de la réalité juridique qui pourra, par la suite, faire l'objet d'une évaluation ou d'une critique. Il sera ainsi possible pour les auteurs qui adoptent une perspective normative d'identifier certaines lacunes ou certaines problématiques relativement à la réalité juridique observée, et de se prononcer sur la nécessité de faire évoluer le droit de manière à résoudre ces problèmes. Contrairement aux théoriciens qui adoptent une perspective descriptive, ces auteurs posent un jugement de valeur sur la réalité juridique qu'ils observent et proposent d'amender. (Benyekhlef et Déziel, 2018, p. 20)

Cette façon de distinguer les différentes conceptions de la protection de la vie privée s'apparente à celle proposée par Alan Moore (citée par DeCew) : « A descriptive or non-normative account describes a state or condition where privacy obtains. […] A normative account, on the other hand, makes references to moral obligations or claims. » (DeCew, 2018; Moore, 2008, p. 412-413) Elle rejoint également les propos d'Helen Nissenbaum, qui abonde dans un sens similaire :

> Some authors have argued that confusion over the concept of privacy arises from a failure to recognize the difference between descriptive or neutral conceptions and normative ones. To provide a neutral conception is to state what privacy is without incorporating into its meaning that privacy is a good thing, worth having, and deserving moral and legal protection. A normative conception of privacy, by contrast, incorporates a presumption that privacy is something worthwhile, valuable, and deserving of protection. (Nissenbaum, 2009, p. 68)

Il est donc possible de distinguer les différentes conceptions de la protection de la vie privée selon qu'elles décrivent la situation de la « vie privée » dans un espace-temps particulier (comme le ferait un historien ou un anthropologue, par exemple) ou dans un système juridique particulier (comme certains juristes le font). Il est également possible de le faire selon le fait qu'elles visent à définir un idéal de la protection de vie privée (comme peuvent le faire les philosophes ou les juristes lorsqu'ils font des propositions pour améliorer les systèmes juridiques existants).

Une autre façon de qualifier les différentes conceptions de la vie privée est celle présentée par DeCew. Cette dernière qualifie les différentes conceptions de la protection de la vie privée selon qu'elles approchent cette question d'un point de vue *réductionniste* ou d'un point de vue *cohérentiste* :

> Reductionists are generally critical of privacy, while coherentists defend the coherent fundamental value of privacy interests. […] [Reductionists] view what are called privacy concerns as analyzable or reducible to claims of other sorts, such as infliction of emotional distress or property interests. They deny that there is anything useful in considering privacy as a separate concept. They conclude, then, that there is nothing coherent, distinctive or illuminating about privacy interests. On the other side, more theorists have argued that there is something fundamental and distinctive and coherent about the various claims that have been called privacy interests. On this view, privacy has value as a coherent and fundamental concept, and most individuals recognize it as a useful concept as well. Those who endorse this view may be called *coherentists*. Nevertheless, it is important to recognize that coherentists have quite diverse, and sometimes overlapping, views on what it is that is distinctive about privacy and what links diverse privacy claims. (DeCew, 2018)

Les positions réductionnistes mettent en doute l'existence même d'un droit à la protection de la vie privée. La philosophe Judith Jarvis Thomson s'inscrit dans cette catégorie. Elle prétend que la protection de la vie privée n'est qu'un terme qui désigne un agrégat (« cluster ») de droits apparentés, mais distincts. Cette parenté entre les droits donne une impression d'unité, mais elle ne serait pas fondée en raison, chacun de ces droits pouvant être opérationnalisé sans qu'il y ait besoin de faire référence à quelque chose comme « la protection de la vie privée ». À ce sujet, Jarvis Thomson écrit :

> 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. (1975, p. 313)

Jarvis Thomson poursuit en donnant quelques exemples, dont les suivants : si l'on vous torture pour vous faire dire quelque chose, ce n'est pas votre vie privée qui est atteinte, mais bien votre droit de ne pas être torturé. Si l'on vous épie au travers des murs à l'aide d'une machine à rayon X, ce n'est pas votre vie privée qui est atteinte, mais votre droit de ne pas voir quelqu'un empiéter votre propriété privée. Bien que la pertinence de cet exemple précis puisse être remise en question, la position réductionniste demeure certainement défendable et plausible. De l'autre côté, les théoriciens cohérentistes estiment que le droit à la protection de la vie privée existe. Ils lui accordent volontiers une pertinence théorique et la défendent à ce titre.

En plus de proposer une distinction entre conceptions *descriptives/normatives*, Benyekhlef et Déziel (2018) utilisent des critères similaires à ceux proposés par DeCew. Ils distinguent les conceptions de la protection de la vie privée selon qu'elles lui accordent une valeur *en soi* (une valeur *intrinsèque*) ou qu'elles lui accordent le statut de m*oyen en vue d'atteindre une autre finalité* (valeur *instrumentale*). Le chercheur Neil Richards — qui, comme nous le verrons plus loin, pour des raisons purement stratégiques préfère miser sur la valeur instrumentale de la protection de la vie privée — décrit ainsi les positions qui accordent une valeur intrinsèque à la protection de la vie privée :

> Many people believe privacy to be a good thing in itself. Many, for example, believe that having places we can go – a forest, a library, a bedroom – without being observed is good without further justification. Being alone and unobserved can be seen as (as a philosopher would put it) an intrinsic good. Intrinsic goods are things that are good in and of themselves, in a way that is separate from any other consequences they produce. They are fundamentally good things, and they are ends in themselves. (Richards, 2022, p. 67)

Il existerait sans doute d'autres moyens de classifier les différentes théories de la protection de la vie privée, mais il ne paraît pas essentiel d'aller plus loin à ce stade-ci de mon travail de recherche. L'idée était simplement d'offrir un premier regard sur la complexité qui s'offre à la personne qui décide d'aborder la question de la protection de la vie privée.

2.2.2 Certaines conceptions traditionnelles de la protection de la vie privée

Dans les faits, c'est un lieu commun d'entamer un texte portant sur la protection de la vie privée en mettant en lumière la confusion entourant le concept (Richards, 2022, p. 17). La définition, la portée et la valeur de la vie privée et du droit qui en découle souffrent d'un déficit d'unanimité, c'est un fait largement reconnu. Judith Jarvis Thomson (1975) faisait déjà état de cette situation : « Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is. » Pour les juristes Ignacio Cofone et Adriana Robertson, la situation visée par ce constat de Thomson aurait peu évolué depuis son énonciation (Cofone et Robertson, 2018). Pour Macnish, « the exact definition and limits of privacy are highly disputed » (2019, p. 5). Pour Nissenbaum, il existe au moins une certitude sur la vie privée : « One point in which there seems to be near-unanimous agreement is that privacy is a messy and complex subject. » (2009, p. 67) Finn, Wright et Friedewald soulignent que « "privacy" has proved notoriously difficult to define » (2013, p. 2). Pour Daniel Solove, la protection de la vie privée est tout simplement « un concept en désarroi » (2008, p. 1-2). Dans un registre moins emphatique et plus près de nous, Benyekhlef et Déziel concluent de leur côté que « la vie privée est un concept complexe faisant l'objet d'analyses, d'interprétations et d'efforts théoriques variés » (2018, p. 75). Pour Debbie Kasper, la raison de ce cul-de-sac théorique est la suivante : « Scholars tend to define privacy as understood within their specific research. As a result, their notions of privacy are limited, and they remain unable to capture its broader meaning. » (2005, p. 74)

Il est coutumier de poursuivre en dressant un florilège des principales approches théoriques dont elle a fait l'objet au courant du dernier siècle. D'emblée, la protection de la

vie privée est un concept difficile à cerner, mais son usage est pourtant largement répandu dans le langage courant. Les dictionnaires peuvent nous aider à débroussailler le terrain conceptuellement. Pour l'Office québécois de la langue française, la « vie privée » est l'« [e]nsemble des phénomènes qui sont personnels, tant sur le plan physique que mental » (OQLF, 2002). Cette définition n'épuise en rien le sujet, car elle laisse ouverte la question de déterminer quels sont les phénomènes physiques ou mentaux qui sont dits « personnels ». En outre, sa portée semble si large qu'elle permet d'inclure des éléments qui relèvent de la psychologie (les pathologies psychologiques par exemple, qui sont des phénomènes mentaux) ou de l'anthropologie philosophique (les questions concernant la nature de la conscience et des perceptions, par exemple). Il semble peu probable que les mécanismes juridiques de protection de la vie privée visent à protéger l'ensemble de ces phénomènes mentaux. *Le Petit Robert* permet de faire un tour d'horizon plus précis. On y voit d'abord que le mot « vie » s'entend de multiples façons. À l'intérieur de toutes les définitions que l'on retrouve dans ce dictionnaire, le sens qui s'approcherait le plus de ce que l'on entend dans l'expression « vie privée » serait peut-être celui-ci : « Part de l'activité humaine, type d'activité qui s'exerce dans certaines conditions, dans certains domaines. » L'ajout de l'épithète « privé » vient clarifier de quelle « part de l'activité humaine » il est question quand nous pensons à la vie privée. Ainsi, *Le Petit Robert* définit le terme « privé » selon huit sens différents : « Où le public n'a pas accès »; « à laquelle n'assistent que les intimes »; « qui se déroule à part »; « seul à seul »; « individuellement »; « intime »; « qui n'a aucune part aux affaires publiques »; et, finalement, « qui ne dépend pas de l'État ».

Ce jeu du dictionnaire met en lumière plusieurs aspects que l'on prête volontiers à la vie privée : la nature *individuelle* de cette chose par opposition à ce qui est *collectif*; un lien évident avec les notions *d'intimité* et de *solitude*; la *mise en disponibilité volontaire et choisie* de certains aspects de notre existence et de notre histoire personnelle et *l'accessibilité contrôlée* à notre personne, à notre corps, à nos pensées ou aux informations qui découlent de nous et de nos actions; la *distinction* que nous opérons entre des biens qui sont dits « publics » (ce qui est à tous) par rapport aux biens « privés » (ce qui est à soi); et, finalement, la *non-interférence de l'État* dans les actions des individus. Ce petit exercice montre

d'emblée la pluralité des sens qui sont associés communément à l'expression « vie privée ». S'il s'avère insatisfaisant du point de vue théorique, il laisse toutefois entrevoir un horizon de sens possibles. Si ce terme couvre de nombreuses significations dans le langage commun, il en va tout autant pour les théoriciens qui n'ont pas été à ce jour capables de fournir une définition claire et univoque de ce qui doit être entendu par « protection de la vie privée ». Voyons désormais quelques-uns des sens qui lui ont été octroyés au fil du temps.

J'ai déjà fait mention de l'ouvrage *Understanding Privacy* de Solove dans le premier chapitre de ce mémoire. J'y reviens, car Solove propose une recension des principales conceptions du droit à la protection de la vie privée qui ont été avancées par un ou plusieurs théoriciens au courant du siècle dernier (Solove, 2002, 2006, 2008). Selon lui, ces conceptions ont eu en commun d'avoir été échafaudées à partir d'une « méthode traditionnelle » : « Under what I will refer to as the "traditional method", conceptualizing privacy is understood as an attempt to articulate what separates privacy from other things and what identifies it in its various manifestations. » (Solove, 2008, p. 13)[26] La méthode traditionnelle consiste simplement à définir ce qui caractérise la protection de la vie privée et à trouver ce qui la distingue des phénomènes qui pourraient s'y apparenter. Les conceptions qui découleront de l'application de la méthode traditionnelle sont en fait celles que DeCew qualifie de cohérentistes. Il y aurait selon Solove six grandes familles de conceptions théoriques du droit à la protection de la vie privée qui auraient été produites à partir de cette méthode traditionnelle. Ce droit aura été compris coup sur coup comme : un droit *à être laissé seul* (« The right to be left alone »); un droit *à gérer l'accès à sa personne* (« Limited Access to the Self »); un droit *au secret et la confidentialité* (« Secrecy »); un droit au *contrôle de ses renseignements personnels* (« Control over Personnal Information »); un droit à *la protection de l'identité individuelle* (« Personhood »); et finalement un droit à *l'intimité* (« Intimacy »).

[26] Solove oppose sa propre méthodologie d'inspiration wittgensteinienne et pragmatiste à cette méthode dite « traditionnelle ». Voir à ce sujet la section 1.4.3.

Le droit *à être laissé seul* correspond en fait à l'idée proposée par Warren et Brandeis dans leur texte canonique paru en 1890 et dont j'ai déjà fait mention. Dans leur article, ces juristes faisaient du droit à la protection de la vie privée un droit à pouvoir vaquer à ses occupations sans craindre une intrusion externe dans un espace privé de vie (par exemple, à l'intérieur de l'enceinte d'une maison). Pensons entre autres à la prise non consentie de photos et à la diffusion d'informations à large échelle, notamment par le biais des médias écrits.

La protection de la vie privée entendue comme un droit à *limiter l'accès à sa personne* s'apparente au *droit d'être laissé seul*, mais les auteurs qui sont rattachés à cette école de pensée élargissent les notions de solitude et d'isolement pour y inclure également le droit d'être laissé libre de l'interférence d'agents extérieurs dans la conduite de ses affaires de façon plus générale. L'intrusion gouvernementale est un exemple patent de ce qui est entendu ici par les auteurs. Ainsi, le droit à la protection de la vie privée est perçu comme un droit de limiter l'incidence que d'autres peuvent avoir sur les processus de prise de décision et sur le choix autonome d'un projet personnel de vie. Comme le précise Solove :

> The limited-access conception is not equivalent to solitude. Solitude is a form of seclusion, of withdrawal from other individuals, of being alone. Solitude is a component of limited-access conceptions, as well as of the right-to-be-let-alone conception, but these theories [celles du « Limited Access to the Self »] extend far more broadly than solitude, embracing freedom from government interference, as well as from intrusions by the press and others. Limited-access conceptions recognize that privacy extends beyond merely being apart from others. (2008, p. 19)

La protection de la vie privée entendue comme un droit *au secret ou à la confidentialité* prévoit qu'une personne peut s'attendre à ce que l'information qui la concerne demeure confidentielle. En contrepartie, ce droit génère une obligation pour le tiers qui doit préserver cette confidentialité qui suit l'information et ne disparaît pas malgré la divulgation initiée par la personne concernée. En fait, selon Solove, cette conception du droit à la vie privée s'apparente au droit à la confidentialité tel qu'il existe dans le monde des affaires. Elle repose sur l'idée qu'il existe une valeur économique et stratégique à cacher certaines informations, tout comme il peut exister un avantage concurrentiel pour un tiers à les connaître.

La protection de la vie privée comprise comme étant un droit au *contrôle de ses renseignements personnels* (« *Control over Personnal Information* ») est présentée par Solove comme une extension des conceptions précédentes. Elle est basée sur l'idée de considérer le renseignement personnel comme une extension de la personne à laquelle il est rattaché. Le fait de protéger la vie privée consisterait donc à permettre à la personne concernée par un renseignement de gérer l'accès à celui-ci (de la même façon qu'elle peut gérer l'accès à sa personne) et de lui garantir la confidentialité de ces renseignements (lorsqu'elle le réclame ou peut s'attendre à ce qu'elle soit garantie). Il s'agit donc d'assurer la gestion de l'accès aux renseignements (comme le fait de limiter l'accès à sa personne à des individus ou des entités déterminés, idéalement de façon libre et consentie). La plupart des lois et des mécanismes de protection des renseignements personnels existants s'appuient sur une telle conception de la vie privée.

La cinquième conception identifiée par Solove est entendue comme un droit à *la protection de la personnalité* (« Personhood »), c'est-à-dire qu'elle consisterait à protéger un espace à l'intérieur duquel la personne peut s'épanouir, où elle peut exprimer son individualité. Solove identifie finalement un sixième regroupement de conceptions théoriques qu'il associe au terme « *Intimacy* ». Les théories visées par ce sixième regroupement font de la protection de la vie privée un droit à *l'intimité* entendu comme la mise en place et la protection d'espaces ou d'enclaves d'intimité permettant à des personnes d'édifier des relations interpersonnelles.

Solove précise que la protection de la vie privée entendue comme étant une *protection de la personnalité* « differs from the theories discussed earlier because it is constructed around a normative end of privacy, namely, the protection of the integrity of the person » (Solove, 2008, p. 30). Cette précision pourrait tout autant s'appliquer aux approches dites de l'*intimité*. Ces deux derniers regroupements d'approches théoriques s'inscrivent ainsi dans une perspective différente des quatre premières. Au lieu de cerner et de définir ce qui distingue la protection de la vie privée en elle-même, elles appuient plutôt cette distinction sur une finalité visée par la mise en place de la protection de la vie privée et qui fait appel

explicitement à des considérations éthiques. Elles renvoient à une idée qui fait de la protection de la vie privée un instrument en vue de protéger autre chose, cet « autre chose » étant quelque chose qui est valorisé dans nos sociétés libérales occidentales. Je reviens de façon plus élaborée sur la dimension instrumentale de la protection de la vie privée dans la section 2.4.

Pour Solove, ces conceptions de la protection de la vie privée sont toutes lacunaires à leur façon. Elles échouent toutes à rendre compte adéquatement de la réalité couverte par ce que nous entendons généralement par l'expression « vie privée » :

> The most prevalent problem with conceptions is that they are either too narrow because they fail to include the aspects of life we typically view as private or too broad because they fail to exclude matters that we do not deem private. Some conceptions even suffer from being both too narrow and too broad. (2008, p. 13)

C'est pourquoi Solove ne cherche plus à définir la protection de la vie privée à partir d'une caractéristique centrale, mais tente plutôt de produire des taxonomies qui pourraient rendre compte de la complexité de cette notion, comme nous l'avons vu dans le premier chapitre.

2.3 *CARACTÉRISER LA PROTECTION DE LA VIE PRIVÉE*

2.3.1 Les approches taxonomistes ou typologiques de la vie privée

J'ai déjà présenté les taxonomies des risques et des préjudices portés à la vie privée élaborées par Solove et de Keats Citron à la section 1.4.3. Ils ne sont cependant pas les seuls auteurs contemporains à aborder la question de la protection de la vie privée en établissant une taxonomie ou une typologie[27]. À titre d'exemple, Finn, Wright et Friedewald ont proposé d'établir une taxonomie des types de protection de la vie privée (Finn *et al.*, 2013; Gutwirth

[27] La taxonomie diffère de la typologie principalement à partir de la méthode utilisée pour la produire. Alors que la taxonomie utilise une approche inductive et émerge naturellement à partir des données, se définit comme un ensemble de configurations empiriques et est construite à partir d'une base de données formelle et de techniques analytiques quantitatives, la typologie est déductive et « se définit comme un ensemble de configurations conceptuelles définies a priori à partir d'attributs multiples » (Borgès Da Silva, 2013).

et al., 2011). Ils s'attardent à déterminer les différentes dimensions de la vie privée qui, selon eux, doivent être protégées par les politiques et les mécanismes juridiques entourant la vie privée. Dans les faits, leur proposition reprend et étend une classification produite antérieurement par Roger Clarke à la fin des années 90 (Clarke, 1997). Finn, Wright et Friedewald ajoutent trois dimensions au modèle de Clarke qui en comprenait quatre, et ce, pour tenir compte des avancées technologiques qui ont émergé depuis la parution de son article en 1997. Les sept dimensions de la vie privée identifiées par ces chercheurs sont :

1) la dimension corporelle[28] (« privacy of the person » – le fait de préserver le caractère privé du corps, de ses mesures et de ses fonctions [ex. les données biométriques[29]]);

2) la dimension se rapportant aux comportements et aux actions de la personne (« privacy of behaviour and action » – le fait de préserver le caractère privé de son orientation sexuelle, de ses affiliations politiques, de ses croyances religieuses, etc.);

3) la dimension communicationnelle (« privacy of communications » – le fait de se prémunir contre l'interception de ses échanges avec les autres, contre l'écoute illicite);

4) la dimension informationnelle et se rapportant à l'image de la personne (« privacy of data and image » – le fait de protéger l'accès aux données et aux images);

[28] Entendu comme la protection du corps et de l'intégrité physique de la personne.

[29] Sont biométriques les données tirées à partir de l'« analyse mathématique des caractéristiques uniques d'une personne, afin de déterminer ou de prouver son identité » (OQLF, 2020a). Sous cette catégorie, nous pouvons considérer les données morphologiques (par exemple, la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil, etc.), les données comportementales (par exemple le tracé de la signature, l'empreinte de la voix, la démarche, la façon de taper sur un clavier, etc.) et les données biologiques (par exemple, l'ADN, le sang, la salive, l'urine, les odeurs, etc.) (CAI, 2022a). Les limites de ce qui peut être considéré comme une donnée biométrique ne sont pas si claires qu'il peut en paraître, notamment parce que le recours à l'intelligence artificielle permet désormais d'inférer l'identité d'une personne à partir de données corporelles très variées.

5) la dimension se rapportant aux pensées et aux sentiments (« privacy of thoughts and feelings » – le fait de tenir pour soi son opinion ou ses émotions);

6) la dimension se rapportant à la localisation et à l'occupation de l'espace [privé] (« privacy of location and space » – le droit de se mouvoir à sa guise dans l'espace public, sans crainte d'être identifié ou suivi); et, finalement

7) la dimension concernant le caractère privé de certaines associations entre personnes (« privacy of association » – le fait de s'associer librement avec autrui)[30].

Finn, Wright et Friedewald élaborent leur taxonomie à partir d'une analyse des répercussions que certaines nouvelles technologies ont sur la protection de la vie privée. Par exemple, certains algorithmes d'intelligence artificielle permettent désormais de déduire les états mentaux des individus à partir des nuages de données récoltées et produites par la quantité croissante de capteurs, notamment par les objets connectés. L'existence de ces algorithmes justifierait, selon les chercheurs, l'ajout de la dimension de la protection de la vie privée se rapportant aux comportements et aux actions de la personne et celle se rapportant aux pensées et aux sentiments.

Dirigé par Bert-Jaap Koops, un autre groupe de six chercheurs a proposé une typologie plus exhaustive de la vie privée (Koops *et al.*, 2017). Celle-ci s'appuie sur une recherche documentaire effectuée sur trois catégories de sources d'information soit : les tentatives antérieures de classification de la vie privée[31]; les constitutions de neuf pays choisis selon des critères précisés dans la recherche; et la littérature scientifique produite par les chercheurs de ces neuf pays au sujet de leur constitution et du traitement qui est fait de la vie privée dans celles-ci. À partir des différentes manifestations de l'objet « vie privée » dans les documents analysés, les auteurs en viennent à établir une typologie qui présente neuf types de vie privée

[30] Cette dernière dimension de la protection de la vie privée est associée au concept de *protection de la vie privée des groupes* que j'évoque à la section 3.2.2.

31 Ils citent notamment les travaux d'Alan Westin, de Roger Clarke, d'Anita Allen et ceux de Rachel Finn, David Wright et Michael Friedewald (Allen, 2011; Clarke, 2021; Finn *et al.*, 2013; Westin, 1960).

désignés par l'expression « constitutional types of privacy ». Ces types de vie privée renvoient à des dimensions distinctes l'une de l'autre (sauf peut-être pour l'une d'entre elles, car elle recoupe toutes les autres), mais constitutives de la vie privée, c'est-à-dire qu'elles lui sont généralement rattachées conceptuellement. Les huit premiers types sont :

- *la vie privée corporelle* (« bodily privacy ») : il s'agit de l'intérêt d'une personne à limiter l'accès à son corps.

- *la vie privée intellectuelle* (« intellectual privacy ») : il s'agit de l'intérêt des personnes à jouir d'une liberté de penser, d'avoir des opinions, des idées et des croyances.

- *la vie privée spatiale* (« spatial privacy ») : il s'agit de l'intérêt d'une personne à pouvoir jouir d'un espace privé de proximité, qui lui est propre (par exemple avoir une chambre ou une demeure).

- *la vie privée décisionnelle* (« decisional privacy ») : il s'agit de l'intérêt d'une personne à pouvoir s'engager dans une activité plus sensible ou très intime, à l'abri du regard des autres (par exemple, la liberté de s'engager dans des activités sexuelles ou d'obtenir un avortement).

- *la vie privée communicationnelle* (« communicational privacy ») : il s'agit de l'intérêt d'une personne à pouvoir exercer un certain contrôle sur les communications qu'elle entretient avec des tiers.

- *la vie privée associative* (« associational privacy ») : il s'agit de l'intérêt d'une personne à pouvoir déterminer avec qui elle veut entretenir des relations.

- *la vie privée possessionnelle* (« proprietary privacy ») : il s'agit de l'intérêt d'une personne à pouvoir user de certains objets ou de pouvoir jouir d'un espace (par exemple, une maison, un paravent, un bureau fermé, etc.) lui permettant de préserver la confidentialité de certains faits ou gestes aux yeux du public en général.

- *la vie privée comportementale (*« behavioral privacy ») : il s'agit de l'intérêt d'une personne à pouvoir conduire des activités en public sans subir le regard constant des autres, c'est-à-dire d'avoir la capacité d'être « soi-même » dans un espace public.

À ces huit catégories, ils en ajoutent une neuvième qui les recoupe et leur est transversale. Il s'agit de *la vie privée informationnelle* (« informational privacy »), similaire en son contenu à l'idée de protection des renseignements personnels. Pour ces auteurs, la protection de la vie privée informationnelle transcende et surplombe toutes les autres catégories de protection de la vie privée. En effet, chacune des dimensions de la vie privée mentionnées dans leur typologie est susceptible de donner lieu à une production d'informations qui touchent, de ce fait, à la dimension informationnelle de la vie d'une personne. Par exemple, les photographies du corps d'une personne ou les données biométriques qui sont extraites d'un moniteur d'activités de type « fitbit » sont autant de données rattachées à la dimension corporelle de la protection de la vie privée. Les données de géolocalisation générées automatiquement par un téléphone cellulaire sont en lien avec la dimension spatiale de la vie privée. Les communications échangées par le biais de ce même téléphone et les métadonnées qui y sont associées sont autant de renseignements rattachés aux dimensions communicationnelle (le message lui-même), associative (l'identité des interlocuteurs) et, potentiellement, décisionnelle (selon le sujet de la discussion) de la vie privée. C'est pourquoi ils font de la dimension informationnelle de la protection de la vie privée une sorte de métadimension.

Les auteurs distribuent les huit premières catégories de vie privée dans une matrice construite autour de trois axes. Ces trois axes représentent trois dimensions théoriques — les auteurs utilisent l'expression « theoretical/doctrinal dimensions of privacy » — à partir desquelles il est possible de qualifier les neuf types constitutifs de la vie privée. Il s'agit en fait de trois spectres différents qui permettent de positionner chacune des catégories de vie privée par rapport aux autres. Le premier spectre situe les dimensions de la vie privée selon qu'elles s'expriment :

- dans un espace qui est totalement personnel (le corps et la pensée);
- dans un espace rappelant l'intimité (l'espace physique avoisinant la personne et l'espace de liberté qui permet de prendre des décisions personnelles);
- dans des espaces semi-publics (l'espace où se déroulent les communications avec autrui et les espaces qui rendent possibles les associations avec autrui); ou
- dans les espaces entièrement publics (l'espace détenu publiquement en vertu d'un droit de propriété privé et l'espace public où il est possible d'afficher des comportements observables par les autres).

Chacun des types de la vie privée est ensuite distribué verticalement selon qu'il exprime une liberté négative (être laissé libre d'interférence externe) ou une liberté positive (avoir la possibilité d'agir librement). Ainsi, alors que la vie privée corporelle s'exprime dans le fait de ne pas subir d'ingérence externe (par exemple, dans le fait de ne pas être contraint à la vaccination), la vie privée intellectuelle s'exprime davantage dans le fait de pouvoir se développer librement (par exemple dans le choix de pouvoir choisir son cursus universitaire). Le troisième axe (représenté par une diagonale dans une illustration que l'on retrouve dans leur article) est un continuum qui part des activités où la protection de cet aspect de la vie privée est davantage axée autour de la gestion de l'accès à cet espace privé (par exemple, gérer l'accès à notre corps) vers la possibilité d'exercer un contrôle une fois que l'accès a été donné (par exemple, avoir la possibilité d'exercer le contrôle sur les propos que nous énonçons ou sur nos actes faits en public). Autrement dit, plus une action se déroule dans un espace public (plus nous nous trouvons à droite sur l'axe horizontal), moins il s'agit d'une situation où l'on gère l'accès à notre vie privée (par exemple, tendre son bras volontairement pour recevoir un vaccin) et plus il s'agit d'une situation où nous assumons un contrôle sur ce que nous en laissons voir aux autres (par exemple, participer ou non à une manifestation en raison de nos opinions politiques).

Les deux typologies de la vie privée présentées ici, auxquelles s'ajoutent également celles de Solove et de Citron présentées à la section 1.4.3, sont des conceptions *descriptives*

de la vie privée. Elles ne tentent pas de définir ce que devrait être la protection de la vie privée, mais s'attardent plutôt à décrire ce qu'elle est actuellement. Elles ont toutefois leur pertinence dans le cadre de ce mémoire, car elles soulignent le caractère multidimensionnel de la vie privée. Si l'objectif d'une évaluation des risques et des préjudices est de protéger la vie privée, elle ne saurait prétendre atteindre celui-ci en ne considérant que sa dimension informationnelle. Même si dans un contexte numérique la dimension informationnelle est primordiale, elle n'épuise pas le domaine d'application de la protection de la vie privée. Autrement dit, même si une organisation peut se limiter à envisager des enjeux liés à la protection des renseignements personnels ou de sécurité de l'information dans ses processus d'évaluation des risques et des préjudices, elle laisse de côté d'importants pans de la protection de la vie privée.

2.3.2 La protection des renseignements personnels en tant que norme liée à l'intégrité contextuelle

La notion *d'attente raisonnable à la vie privée* est souvent évoquée par les juristes et les organismes de surveillance en matière de protection de la vie privée. Il s'agit d'un critère objectif dont ils se sont dotés pour interpréter l'article 8 de la *Charte canadienne des droits et libertés* qui stipule que chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Il vise en fait à établir à quel moment une fouille, une perquisition ou une saisie devient abusive. Rendu dans le cadre d'une affaire de voyeurisme impliquant l'enregistrement vidéo non consenti de jeunes étudiantes en classe, l'arrêt Jarvis de la Cour suprême du Canada met bien en lumière la nature de cette notion :

> Le concept de « vie privée », selon le sens qui y est habituellement donné, n'est pas absolu, et le fait de se trouver dans un lieu public ou semi-public n'entraîne pas automatiquement une renonciation à toute attente de protection en la matière. La question de savoir si une observation ou un enregistrement serait généralement considéré comme une intrusion dans la vie privée dépend plutôt d'un ensemble de facteurs, qui peuvent comprendre le lieu où se trouve la personne, la forme que prend l'intrusion reprochée dans la vie privée, la nature de l'observation ou de l'enregistrement, l'activité à laquelle participe la personne observée ou filmée et la partie du corps de la personne qui est mise à l'avant-plan dans l'enregistrement. Le fait que divers facteurs peuvent influer sur la question de savoir si une personne

> s'attendrait ou non à être observée ou filmée concorde aussi avec le choix du législateur d'exprimer l'élément constitutif de l'infraction par renvoi aux « circonstances » pour lesquelles il existe une attente raisonnable de protection en matière de vie privée. Si le législateur avait eu l'intention de limiter les types de circonstances que le tribunal peut prendre en compte pour décider si l'attente pouvait raisonnablement exister, il l'aurait fait en termes exprès. (*R. c. Jarvis*, 2019)

Dans ce cas, les jeunes femmes étaient filmées dans leur classe et à leur insu par l'enseignant à l'aide d'une caméra dissimulée à l'intérieur d'un stylo. La question de droit mise en cause était « de savoir si les élèves filmées par l'accusé se trouvaient dans des circonstances pour lesquelles il existe une attente raisonnable de protection en matière de vie privée », ce que la Cour suprême confirma à la suite du procès. Ainsi, en droit canadien, la notion de contexte est déjà considérée dans le processus qui permet d'établir ce qui constituerait une atteinte au droit à la vie privée ou non.

L'importance du contexte dans les matières ayant trait à la protection de la vie privée est également au cœur de l'ouvrage *Privacy in Context* d'Helen Nissenbaum paru en 2010. Pour Nissenbaum, l'évaluation de ce qui constitue ou non une atteinte à la vie privée ne peut pas se faire sans prendre en compte le contexte dans lequel l'événement se déroule, parce qu'un contexte particulier engendre une norme de circulation des informations personnelles qui lui est propre[32]. Un exemple : un patient ne s'insurge pas lorsque son médecin de famille lui pose des questions portant sur son mode de vie, il s'y attend même. Ce même patient pourrait voir un problème si son médecin parle de son cas à un membre de sa famille ou à son employeur sans son consentement. Ainsi, il y aurait transgression de la vie privée lorsque l'information sur une personne circule selon un flux informationnel qui ne respecte pas la norme attendue dans le contexte dans lequel cet échange d'information se déroule. Dans une telle situation, elle considère que ce qu'elle nomme l'*intégrité contextuelle* n'est pas respecté : « Contextual integrity is defined in terms of informational norms : it is preserved when informational norms are respected and violated when informational norms are

[32] Nissenbaum s'attarde en effet principalement à des questions de protection de la vie privée informationnelle et moins aux autres formes de vie privée vues dans la section précédente. Ses travaux concernent plus particulièrement la protection de la vie privée dans le contexte des nouvelles technologies.

breached. » (Nissenbaum, 2009, p. 140) Elle utilise l'expression *informational norms* (que je traduis par normes informationnelles) pour désigner une norme propre à un contexte donné et l'expression *context-relative informational norms* (ou normes informationnelles contextuelles) pour désigner ces normes de façon globale.

Le terme « norme » doit être entendu ici dans un sens prescriptif et non dans un sens descriptif. Il ne s'agit pas de décrire un prototype du flux « normal » de l'information dans un contexte donné, mais bien d'énoncer une attente comportementale à l'égard des parties prenantes de ce flux. Par exemple, si l'on constate que la grande majorité des personnes publient des photos sur les réseaux sociaux, on pourrait conclure que la publication de photos est la norme. Or, la norme informationnelle est plutôt une injonction, une prescription ou une attente comportementale quant au flux informationnel attendu dans ce contexte. Même si la plupart des personnes publient des photos sur les réseaux sociaux, cela ne veut pas dire que ces mêmes personnes ne s'attendent pas à conserver un certain contrôle sur la circulation et la diffusion de celles-ci. La norme informationnelle dans ce contexte serait plutôt d'obtenir le consentement préalable avant de réutiliser ou de rediffuser la photo d'un tiers.

La norme informationnelle pour Nissenbaum est structurée par les quatre paramètres suivants : le contexte dans lequel un flux se déroule; les acteurs impliqués; les attributs de l'information mise en cause; et, finalement, le principe de la transmission de l'information. Voici ce qu'elle entend par « contexte » :

> By context, I mean structured social settings with characteristics that have evolved over time (sometimes long period of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more. Familiar to us living in modern industrial societies are contexts of health care, education, employment, religion, family, and the commercial marketplace. (2009, p. 130)

Les acteurs impliqués dans le flux peuvent être le transmetteur de l'information, le récepteur de l'information et l'individu qui est le sujet de l'information (qui peut être également transmetteur ou récepteur de l'information). Les attributs de l'information sont la nature des renseignements impliqués dans un flux (des renseignements financiers, de santé, scolaires, identificatoires, etc.). Finalement, les principes qui sous-tendent la circulation de

l'information sont les éléments centraux qui viennent déterminer si l'intégrité contextuelle est respectée ou non :

> A transmission principle is a constraint on the flow (distribution, dissemination, transmission) of information from party to party in a context. The transmission principle parameter in informational norms expresses in terms and conditions under which such transfers ought (or ought not) to occur. (2009, p. 145)

Nissenbaum donne des exemples concrets de ce qu'elle entend par cette idée de « principe qui sous-tend la circulation de l'information ». Il peut s'agir de la confidentialité (le fait de devoir préserver le secret concernant l'information en circulation); la réciprocité (le fait que l'information doit circuler de façon bidirectionnelle); le mérite (le fait que le récepteur se montre digne de recevoir l'information); l'habilitation (le fait que le récepteur ait le droit de recevoir l'information); la contrainte (le fait que le transmetteur perçoit qu'il est nécessaire de communiquer l'information); et le besoin (le fait que la circulation de l'information réponde à une certaine nécessité) (Nissenbaum, 2009, p. 145). Autrement dit, cette idée de principe énonce certaines qualités qu'une collecte, une utilisation ou une communication de renseignements personnels doit respecter pour être conforme à la norme informationnelle.

Malgré la complexité apparente de sa proposition théorique, il est assez facile de trouver des exemples concrets de normes informationnelles et d'intégrité contextuelle. Dans l'exemple soulevé précédemment concernant des photographies publiées sur les réseaux sociaux, les critères pourraient être exprimés de la manière suivante : le contexte est le réseau social en lui-même (entendu à la fois comme infrastructure technologique et comme écosystème au sein duquel des communications se tiennent); les acteurs impliqués sont les « amis » identifiés dans le réseau; la nature de l'information est constituée par les photographies elles-mêmes[33]; le principe est l'habilitation qu'ont des individus à voir les photographies (par exemple, l'administrateur du réseau social et les « amis » de la personne

[33] Il est facile de voir avec cet exemple en quoi la nature de l'information peut venir influencer la norme informationnelle. Les attentes ne seront pas les mêmes s'il s'agit de photographies de fin de semaine au chalet ou de photographies intimes ou présentant un contenu explicite échangées entre partenaires.

qui ont le droit de voir lesdites photographies). Il y aurait bris de l'intégrité contextuelle du moment où la photographie devient accessible à un tiers. La personne ayant publié initialement la photographie pourrait en effet s'attendre à ce que certaines photos ne circulent pas en dehors de son cercle d'amis, notamment parce qu'elle aurait activé certains paramètres de confidentialité.

L'affaire « Clearview AI » est un bel exemple de bris de l'intégrité contextuelle. Cette compagnie aurait collecté une quantité importante de photographies à l'insu des utilisateurs de nombreux sites populaires (entre autres auprès de Facebook, de YouTube, d'Instagram et de Twitter) dans l'objectif de générer des identifiants biométriques et d'offrir des services d'identification biométriques, notamment aux services policiers. Si les utilisateurs de ces réseaux sociaux pouvaient s'attendre à ce que des tiers consultent des photographies, il y a fort à parier qu'aucun ne s'attendait à ce que ces photos servent éventuellement à des services policiers. L'entreprise a dû cesser ses activités au Canada en raison d'une enquête conjointe du Commissariat à la protection de la vie privée du Canada, de la Commission d'accès à l'information du Québec et de leurs homologues de l'Alberta et de la Colombie-Britannique (CPVPC, 2021). Elle a été également mise à l'amende par *l'Information Commissionner's Office* britannique qui ordonna la destruction de toutes les données collectées sur les sujets britanniques (ICO, 2022).

J'ai aussi déjà évoqué l'exemple de l'information médicale. Il peut sembler naturel pour une personne de communiquer une information médicale à un médecin ou à un membre du personnel du réseau de la santé dans le cadre d'une consultation. À l'intérieur du contexte spécifique d'une prestation de soin médical, il est généralement entendu que la personne (le transmetteur de l'information) peut faire confiance au médecin (le récepteur de l'information) pour recevoir des informations précises sur son état de santé (des informations qui démontrent certains attributs particuliers) parce qu'elle peut s'attendre à ce que la confidentialité de cette information soit préservée et parce qu'il paraît nécessaire que l'information circule pour obtenir un soin de qualité. Dans le contexte québécois, il est normal par ailleurs que le médecin communique certaines informations à la Régie de

l'assurance maladie du Québec (RAMQ) pour des fins de facturation et de remboursement. Le patient s'y attend. En revanche, il y aurait transgression de l'intégrité contextuelle si le même médecin en venait à briser la confidentialité sans le consentement de la personne pour, par exemple, les vendre à des entreprises pharmaceutiques ou pour les communiquer à un employeur. Par ailleurs, cette même personne peut discuter avec un ami proche qui s'avère aussi être médecin. Au courant de la discussion, elle peut lui révéler une information sur son état de santé, mais elle ne s'attend sans doute pas à ce que cette information soit communiquée à la RAMQ. Dans ce deuxième contexte, le principe qui sous-tend la communication d'information n'est plus le besoin médical, mais plutôt le fait qu'elle juge cette personne comme étant digne de confiance et qu'elle a besoin de se confier. Dans les deux cas, toutefois, la confidentialité est un critère qui permet de vérifier si l'intégrité contextuelle est préservée.

En somme, la proposition théorique de Nissenbaum nous renseigne sur la dimension profondément contextuelle de la vie privée informationnelle. En ce sens, sa position se rapproche de l'idée « d'attente raisonnable en matière de vie privée » et de l'interprétation juridique qu'en fait la Cour suprême du Canada. Elle avoue elle-même qu'il existe une certaine parenté entre son concept d'intégrité contextuelle et celui d'attente raisonnable en matière de vie privée (Nissenbaum, 2009, p. 236). Son objectif premier n'est toutefois pas de fonder un quelconque mécanisme juridique pour établir la légalité d'une action, mais plutôt de fournir un critère normatif pour déterminer si un flux informationnel est éthiquement acceptable. La proposition théorique de Nissenbaum met en lumière le caractère hautement contextuel et personnel de ce qui peut être considéré comme une atteinte à la vie privée. Ce qui ressort de son analyse, c'est qu'un flux informationnel ne peut être analysé indépendamment du contexte dans lequel il se réalise. Ainsi, le contexte influence fortement la nature des événements qui pourraient être perçus comme une atteinte portée à la vie privée et les acteurs impliqués jouent un rôle prépondérant dans la perception et dans l'évaluation de l'impact qu'une situation engendre pour la vie privée. Cette contextualité de la notion de « vie privée » milite pour l'adoption d'une définition opérationnelle du risque qui soit, comme le propose Kermisch, à la fois quantitative et qualitative (voir section 1.4.1). Cette

caractéristique de la protection de la vie privée devrait influencer le domaine d'application des processus d'évaluation de gestion des risques. Si l'objectif de l'évaluation des risques et des préjudices (ce qui détermine son domaine d'application) est de protéger la vie privée des personnes impliquées, il semble tout à fait cohérent de privilégier la perspective des personnes visées par la mise en œuvre du projet ou de l'initiative, et non celui de l'organisation qui la réalise. En outre, il faut tenir compte du caractère hautement subjectif de l'appréciation du préjudice à la vie privée : ce qu'une organisation perçoit comme un préjudice mineur peut acquérir une dimension tout autre dans l'œil de celui qui le subit.

2.3.3 La protection de la vie privée en tant que concept essentiellement contesté

Il est dans la nature de certains concepts d'être flou, et ce, même si leur utilisation dans le langage commun est largement répandue. Il en va ainsi des concepts « bien », « justice », « connaissance », « démocratie », « art » ou encore « amour », pour n'en nommer que quelques-uns. C'est en 1956 que le philosophe Walter Bryce Gallie utilisa l'expression *concept essentiellement contesté* pour qualifier ces concepts dont l'« usage suscite inévitablement des disputes interminables concernant leurs usages appropriés de la part de leurs utilisateurs » (Gallie, 2014, p. 11). Plus récemment, trois chercheurs ont tissé un lien entre le concept de « protection de la vie privée » et l'idée de Gallie concernant les *concepts essentiellement contestés*. Ainsi, Mulligan, Koopman et Doty ont analysé le concept de protection de la vie privée à l'aune des sept critères identifiés par Gallie et concluent qu'il s'agit bien d'un *concept essentiellement contesté* (Mulligan *et al.*, 2016).

Pour Gallie, un concept peut être considéré comme étant essentiellement contesté s'il répond aux sept critères suivants :

(I) Il est tenu en estime par ses utilisateurs. Il est « appréciatif [appraisive] au sens où il désigne ou accrédite un type d'accomplissement [achievement] qui est valorisé [valued] » (Gallie, 2014, p. 13).

(II) Il doit faire montre d'une certaine complexité interne, même si « sa valeur lui est attribuée en bloc [as a whole] ». Autrement dit, peu importe le nombre de constituantes internes qu'on lui attribue et la configuration qu'on prête à celles-ci, le concept est estimable pour lui-même.

(III) Il peut être décrit de différentes façons, et ces descriptions varieront en fonction de l'importance accordée à ses constituantes internes et à la hiérarchie qui en découlera. Toutefois, en définitive, peu importe comment il est décrit, « aucune des nombreuses descriptions rivales de sa valeur totale n'est absurde ni contradictoire ». Autrement dit, la coexistence de plusieurs descriptions concurrentes ne discrédite en rien l'usage et l'existence du concept. Chacune de ces descriptions s'explique et se comprend logiquement à partir de ses prémisses. Du critère (III) découle une conséquence (IIIa) : le concept est susceptible d'être ambigu, particulièrement lors de ses premiers usages.

(IV) Il doit admettre « des modifications considérables à la lumière de circonstances changeantes ». Le concept est « ouvert » à la modification dans le temps, selon le contexte dans lequel il évolue.

(V) Les défenseurs d'une acception particulière du concept connaissent et reconnaissent les positions théoriques antagonistes, même s'ils les contestent, et sont conscients que leur propre usage est contesté par d'autres.

Les cinq premiers critères précisent les caractéristiques définitionnelles des concepts essentiellement contestés. Ils ne suffisent toutefois pas selon Gallie pour les distinguer des concepts qui seraient simplement *confus*. Il propose ainsi deux critères supplémentaires :

(VI) Les différentes conceptions dérivent d'un modèle [exemplar] original — ou de modèles [exemplars] reconnus — par toutes les parties qui défendent celles-ci. Autrement dit, les utilisateurs du concept s'entendent pour reconnaître que certaines situations, certains événements ou certains objets sont des instanciations concrètes du concept.

(VII) Les contestations dont le concept fait l'objet contribuent au développement continu de celui-ci et rendent possible le maintien ou le développement de l'accomplissement du modèle original de manière optimale. Autrement dit, le concept *essentiellement contesté* n'est pas simplement un concept qui est confus. Si cela était le cas, les débats viendraient à bout de l'éclaircir. Or, le véritable concept essentiellement contesté est et sera, vraisemblablement, de tout temps contestable, parce qu'il est dans sa nature même de l'être et que les contestations dont il fait l'objet le font évoluer parallèlement à l'évolution du contexte dans lequel il est utilisé (2014, p. 13-14; 19).[34]

Selon Mulligan, Koopman et Doty, le concept de protection de la vie privée répond bien aux sept critères de Gallie. D'abord, il est (I) appréciatif dans la mesure où « typical debates over privacy share the common assumptions that privacy is a good thing to have, that it is good for society or at least for the individual » (Mulligan *et al.*, 2016, p. 5). Comme je l'ai mentionné aux sections 2.2.1 et 2.2.2, de nombreux auteurs ont souligné la complexité du concept de protection de la vie privée (II), et son histoire passée et actuelle démontre bien la coexistence de multiples descriptions dont il fait l'objet (III) :

> Despite a long pedigree, there are ongoing contestations over privacy's objectives, justifications, applications and ongoing relevance for contemporary life. […] Owing to its internal complexity, privacy can be described in multiple ways. (2016, p. 6-7)

Toujours selon Mulligan, Koopman et Doty, le concept de protection de la vie privée est bel et bien « ouvert » dans le sens entendu par Gallie (IV). Le fait que les théoriciens renouvellent

[34] Gallie utilise l'exemple de l'« équipe championne » pour illustrer ces sept critères en action (2014, p. 11-13). Si tous s'entendent pour dire qu'il existe quelque chose comme « le prototype de l'équipe championne au hockey » (comme le furent peut-être jadis les Canadiens de Montréal), les positions peuvent varier sur les raisons qui l'ont menée à ce titre. L'équipe championne l'est-elle en vertu d'une attaque redoutable? D'une défensive à toute épreuve? D'un gardien de but inébranlable? D'un coaching efficace? D'un management prescient? Et si l'équipe championne repose sur un amalgame de toutes ces qualités, dans quelle proportion chacun de ces critères est plus important que les autres? Quel est le critère – ou l'amalgame de critères – qui manque cruellement aux Canadiens depuis plusieurs années et qui leur permettrait d'aspirer à la Coupe Stanley?

constamment les discussions sur sa nature afin de pallier ses limites est une démonstration convaincante de son ouverture :

> The history of privacy exhibits this openness. […] Today, we again face the prospect of an open and transformable concept of privacy. As we described in the Introduction, the 1970s-era guidelines that continue to structure our thinking about privacy are bumping up against powerful new technologies that expose their limits. (2016, p. 7-8)

Les trois chercheurs se satisfont également du fait que la plupart des théoriciens dominant le débat sur la protection de la vie privée sont bien au fait des positions adverses et qu'ils positionnent généralement leurs propres travaux par rapport à celles-ci (V). Même s'ils jugent imprécis le sixième critère de Gallie (VI) — celui concernant le rapport à un modèle original — ils concluent également qu'il existe suffisamment d'exemples de situations qui se rapportent à une idée telle que celle de « protection de la vie privée » pour en faire un concept essentiellement contesté et non un concept simplement confus[35]. Finalement, pour ces chercheurs, le septième critère (VII) — l'apport continu des constations au développement du concept — ne doit pas être appliqué rétrospectivement, mais prospectivement. Il ne s'agit pas de faire l'archéologie du concept pour voir de quelles façons les contestations passées auront modelé les conceptions actuelles. Il faut plutôt appliquer le critère de façon prospective, et ce, « because it concerns downstream consequences of the ongoing contestedness of a concept » (2016, p. 9). Autrement dit, il s'agit d'admettre que le débat concernant la protection de la vie privée n'est pas clos et il faut éviter d'accepter son état actuel comme son état final. D'admettre le débat comme étant clos serait d'admettre que le concept de protection de la vie privée était simplement confus et que cette confusion initiale aurait été finalement éclaircie.

[35] L'application de ce critère fait écho à l'anecdote du juge Stewart ainsi qu'à l'évocation du concept de recoupement par consensus de la CEST mentionnées toutes deux en introduction de ce chapitre. En outre, l'utilisation du concept de « vie privée » par le langage commun renvoie également à plusieurs « modèles » de la « vie privée ». Personnellement, je ne pense pas que la conclusion des trois chercheurs est véritablement problématique.

Cette conclusion mène ces auteurs à proposer une grille d'analyse des théories de la protection de la vie privée qui comprend quatorze « dimensions de contestabilité » qu'ils regroupent sous cinq métadimensions (2016, p. 10-15). Pour eux, il s'agit de dire qu'une conception de la protection de la vie privée peut être contestée sous l'un ou l'autre de ces angles, ou sous plusieurs angles simultanément. Ainsi, une conception de la vie privée peut-être contestée :

- selon certains éléments purement théoriques (« dimensions of theory »), soit selon sa finalité (la nature de la protection que la conception veut voir aménager, par exemple la confidentialité), selon sa justification (les raisons qui justifient la protection), selon les éléments qui sont exclus de sa portée ou selon les modèles [exemplars] qu'elle invoque comme justification;

- du point de vue de ce qu'elle entend protéger (« dimensions of protection »), soit selon les éléments concrets qu'elle cible (ce qui doit être protégé, par exemple le renseignement personnel) ou selon le sujet qui doit bénéficier de la protection;

- du point de vue des préjudices causés (« dimensions of harm »), soit selon la nature d'une action qui viole la vie privée (par exemple l'espionnage), selon l'identité du commettant de cette action ou selon la détermination de tiers pour lesquels la protection doit s'appliquer (par exemple, le fait que les informations de santé d'une personne mineure sont inaccessibles aux parents dès ses 14 ans);

- du point de vue des dispositions dont elle fait la promotion (« dimensions of provision »), soit selon les mécanismes déployés (par exemple, les lois et règlements ou les moyens technologiques qui découlent de son application) ou selon les fournisseurs de la protection (par exemple, le gouvernement ou l'entreprise privée); et finalement

- du point de vue du champ d'application de la protection accordée par la théorie (« dimensions of scope »), soit selon les limites du contexte dans lequel elle

> accorde une protection (contexte social, géographique ou autre), selon la durée pour laquelle la protection sera accordée et selon sa portée (qu'elle soit universelle [applicable à tous, de tout temps], générale [applicable à une population] ou particulière [applicable dans des situations particulières ou à des personnes spécifiques].

Les auteurs soulignent quelques conséquences à identifier la protection de la vie privée comme concept essentiellement contesté. Du lot, je retiens celles-ci : d'abord, les débats théoriques l'entourant sont productifs, mais ils ont peu de chance d'être conclusifs. De ce fait, aucune revue de littérature ne peut prétendre à l'exhaustivité, car une problématique inédite en matière de vie privée est toujours susceptible d'émerger et de venir s'ajouter. Cet état d'incomplétude essentielle est dû au fait que l'évolution technologique s'accompagne nécessairement d'une réévaluation constante des différents constituants conceptuels de l'objet « protection de la vie privée ». Pour Mulligan, Koopman et Doty, il nous faut accepter cette « ouverture » du concept et apprendre à vivre avec celle-ci (2016, p. 9-10). Comme ceux de « démocratie », de « justice », d'« amour » ou d'« art », le concept de « protection de la vie privée » est condamné à être redéfini constamment.

Cette conclusion n'est pas sans conséquence du point de vue normatif. Considérant l'évolution incessante du contexte dans lequel la protection de la vie privée est pensée et réfléchie, tant du point de vue technologique que politique, juridique ou sociologique, les conceptions qui en sont faites sont elles aussi condamnées à être constamment réfléchies et repensées. Aucune école de pensée ne saurait prétendre apporter une réponse définitive. Par la bande, cela veut également dire que les situations ou les événements qui peuvent être considérés comme portant préjudice ou atteinte à la vie privée sont aussi condamnés à être revus et réévalués à la lumière de l'évolution de la conception de la vie privée. Le caractère inachevé du concept de vie privée n'est pas nécessairement négatif en soi. C'est une position défendue également par Finn, Wright et Friedewald :

> We also suggest that the fluidity of privacy as a concept may be an important aspect of its utility, since technological developments may introduce new types of privacy.

> As technologies develop and proliferate, various types of privacy which had not previously been considered or identified as under threat may become compromised. (2013, p. 20)

Ce qu'ils disent en somme, c'est que la protection de la vie privée, pour être utile et pour garder sa pertinence, doit savoir évoluer avec l'évolution technologique. Le risque de demain n'existe probablement pas aujourd'hui, et cela commande d'être précautionneux dans la mise en place de toute nouvelle initiative impliquant la collecte, l'utilisation et la communication de renseignements personnels.

2.4 *VALEUR INTRINSÈQUE ET VALEUR INSTRUMENTALE DE LA VIE PRIVÉE*

2.4.1 Certains « mythes » entourant la valeur de la protection de la vie privée

Le fait de prétendre que la vie privée a une valeur intrinsèque peut paraître aller de soi, particulièrement dans notre société québécoise où elle est portée au rang de droit de la personne. Cette idée rencontre cependant certaines objections sur son chemin. D'abord, comme il a été évoqué précédemment, certains défendent des propositions réductionnistes à l'égard de la vie privée et rejettent l'idée même que la protection de la vie privée soit quelque chose en soi, comme le suggère Judith Jarvis Thomson. La non-existence potentielle de quelque chose demeure un obstacle plutôt important au fait de lui accorder une certaine valeur intrinsèque. On pourrait également faire l'objection que certaines personnes entretiennent l'idée que la protection de la vie privée est un concept suranné. En effet, la « mort de la vie privée » ou sa lente agonie est annoncée depuis plusieurs décennies (Johnson, 2010; Sprenger, 1999). La pertinence du concept de « vie privée » est souvent remise en question par le fait que tous se disent concernés et inquiets par rapport à la protection de leur vie privée tout en adoptant des comportements en ligne qui entrent en contradiction avec cette préoccupation autoproclamée. Ce phénomène porte le nom du « paradoxe de la vie privée ». Des exemples patents de cette attitude contradictoire sont la diffusion insouciante et tous azimuts de photos et de renseignements personnels sur les différents réseaux sociaux ou l'augmentation de la consommation sur des sites transactionnels qui sont d'importants

générateurs de données sur les utilisateurs. (Barth et de Jong, 2017; Solove, 2020). Finalement, d'autres sont enclins à penser qu'il n'y a pas d'utilité quelconque à protéger la vie privée, considérant qu'ils n'ont rien de préjudiciable à cacher. Il s'agit du « nothing to hide argument » qui consiste à dire que parce que je n'ai rien fait de « mal », je n'ai pas besoin de voir à ce que les renseignements qui me concernent ne soient pas collectés, utilisés ou communiqués (Cofone, 2019; Solove, 2007).

Pour plusieurs, ces objections et ces dénonciations concernant la vie privée sont à rejeter. D'abord, devant les positions réductionnistes, il est possible d'adopter une position « agnostique ». C'est dire que, même si la protection de la vie privée pourrait ne s'avérer n'être rien dans l'absolu, les discussions l'entourant ne perdent pas pour autant leur utilité pratique dans nos sociétés. Il est aussi possible de remettre en question l'idée que la protection de la vie privée est morte ou mourante. Au contraire, d'un point de vue empirique, l'importance qu'elle occupe dans les débats entourant les nouvelles technologies milite plutôt en faveur de son dynamisme. Pour Neil Richards, l'énonciation de cette présumée « mort de la vie privée » relèverait davantage de l'expression d'une anxiété générée devant la difficulté que certaines personnes éprouvent à protéger adéquatement leurs renseignements personnels dans un contexte technologique en ébullition. En outre, il considère que cette proclamation sert plutôt les intérêts d'une poignée d'industriels pour qui cette « chronique d'une mort annoncée » permet de réduire les attentes en matière de protection de la vie privée de leur clientèle potentielle : « Assertions that Privacy Is Dying are often no more than self-interested framings of the issue by the people and entities who have much to gain from diminished privacy expectations. » (2022, p. 108)

L'existence du paradoxe de la vie privée ne saurait être une preuve que la protection de la vie privée est inutile, ni même qu'elle n'importe pas pour les individus. Pour Daniel Solove, le lien entre la valeur de la vie privée et l'attitude des gens devant leur rapport à leur propre vie privée n'est pas pertinent. Il estime plutôt que les individus abordent la question de la vie privée avec une attitude qui s'apparente à la gestion de leur propre risque : « The privacy paradox is best interpreted not as an indication of how much people value privacy.

Instead, the phenomenon demonstrates behavior involving risk, where many factors might influence people's decisions. » (Solove, 2020, p. 41) Autrement dit, les individus ne considèrent peut-être pas — peut-être de façon erronée — que leur propre vie privée est en danger lorsqu'ils interagissent avec les outils numériques. Richards réitère pour sa part que les personnes sont généralement dépassées par la rapidité avec laquelle les nouvelles technologies sont déployées et pourraient ne pas prendre la pleine mesure des dangers inhérents à leur usage, ce qui peut expliquer également l'existence du paradoxe. En effet, tous ne prennent pas conscience simultanément des risques et des enjeux soulevés par de nouvelles technologies[36]. En outre, il souligne que le paradoxe peut également être inversé : si les personnes ne se préoccupent pas de leur vie privée, pourquoi est-elle un sujet si important pour que nous en parlions tant? Finalement, le « nothing to hide argument » peut être assez facilement démenti. Solove souligne que « [t]he deeper problem with the nothing to hide argument is that it myopically views privacy as a form of concealment or secrecy » (Solove, 2007, p. 764). Autrement dit, étant donné que la protection de la vie privée ne se limite généralement pas à des considérations de confidentialité et de secret (ce que la section 2.2 a rappelé), je ne peux pas conclure qu'elle n'est pas utile ou qu'elle n'a pas de valeur du simple fait que je n'ai personnellement aucune information à cacher. En plus d'être en accord avec cet argument, Richards et Carissa Véliz ajoutent également que cet argument évacue la dimension sociale ou collective de la protection de la vie privée (Richards, 2022, p. 72-79; Véliz, 2020, p. 71-75). En effet, même si individuellement je pense ne rien avoir à cacher, il se peut que l'information que *je* diffuse ou que *je* génère puisse causer un préjudice à un tiers, par exemple si je diffuse une photographie sans le consentement d'un tiers qui figure sur cette photographie. Ces considérations sur l'aspect collectif de la protection de la vie privée sont également soulevées par Véliz :

> Privacy is collective in at least two ways. It's not only that your privacy slips can facilitate violations of the right to privacy of other people. It's also that the consequences of losses of privacy are experienced collectively. A culture of

[36] J'ai aussi évoqué précédemment un autre mythe auquel Neil Richards s'attaque, celui qui traite de la possibilité du contrôle et du consentement véritable dans un contexte technologique (voir page 26).

> exposure damage society. It hurts the social fabric, threatens national security […], allows for discrimination, and endangers democracy. (2020, p. 79)

La philosophe précise et exemplifie sa pensée dans un article paru antérieurement :

> Because we are intertwined in ways that make us vulnerable to each other, we are responsible for each other's privacy. I might, for instance, be extremely careful with my phone number and physical address. But if you have me as a contact in your mobile phone and then give access to companies to that phone, my privacy will be at risk regardless of the precautions I have taken. This is why you shouldn't store more sensitive data than necessary in your address book, post photos of others without their permission, or even expose your own privacy unnecessarily. (2019, s. p.)

Pour conclure sur cet aspect collectif de la protection de la vie privée, Véliz établit un parallèle entre celle-ci et les considérations environnementales : peu importe le souci apporté par une personne quant à son empreinte carbone et les choix de consommation qu'elle fait en ce sens, elle souffrira autant des mauvais choix de ses voisins et compatriotes si ces derniers n'en font pas autant (2020, p. 75-76). De la même façon, toute personne qui agit de manière inconsciente par rapport aux impacts des choix qu'elle prend et des actions qu'elle fait à l'égard de sa propre vie privée peut nuire aux efforts faits par une autre personne.

Du reste, la perspective temporelle peut remettre en question la pertinence de cet argument. Il se peut que je n'aie rien à cacher pour l'*instant*, mais que *je ne sache pas en ce moment que j'aurai quelque chose à cacher dans le futur*. Autrement dit, du point de vue des conditions politiques, sociales ou juridiques actuelles, il est possible que les informations qui circulent au sujet d'une personne ne soient pas préjudiciables, mais rien ne garantit que ces conditions perdurent. Il existe un exemple classique — souvent repris par les chercheurs, et notamment par Véliz (2020, p. 110-114) — d'une telle situation où les individus ne savaient pas au moment X où leurs données ont été collectées que cette collecte leur serait (hautement) préjudiciable au moment Y. Il s'agit de celui du recensement des populations par les autorités hollandaises dans les années 40 visant à rendre possible l'émission d'une carte d'identité. Dans le lot des informations collectées et affichées sur la carte d'identité figuraient, notamment, l'appartenance à la communauté juive. Cette information est, éventuellement,

tombée dans les mains des nazis. La collecte d'information sur l'affiliation religieuse pouvait paraître banale aux moments où elle fut faite, mais celle-ci a pris une tout autre couleur à la lumière des faits qui ont suivi. 73 % des Juifs hollandais auront été tués sous le régime nazi, contre 25 % des Juifs français. Les autorités françaises ne collectaient pas cette information pour des raisons, justement, de protection de la vie privée. Un exemple plus récent, et pour lequel nous ne connaissons pas encore les conséquences, est celui de la collecte de renseignements biométriques par les forces armées américaines auprès de leurs collaborateurs afghans. D'abord collectées pour des raisons purement opérationnelles, il semble que ces données biométriques puissent être tombées entre les mains des forces talibanes au moment de leur reprise du contrôle de l'Afghanistan, signant potentiellement l'arrêt de mort de ces personnes (Chandran, 2021; Hu, 2021). L'actualité récente américaine nous fournit un autre bel exemple en lien avec la défense du droit à l'avortement. Je reviens un peu plus loin sur cet événement spécifique.

Ainsi, malgré certaines voies divergentes au tableau, il semble assez raisonnable de penser qu'une majorité considère que la vie privée est quelque chose de généralement bon et souhaitable. Les législateurs dans le monde n'auront d'ailleurs pas attendu un consensus sur la définition et l'étendue de la vie privée pour mettre en place des mécanismes juridiques pour protéger la vie privée de leurs citoyennes et citoyens.

Neil Richards est d'avis que la vie privée est quelque chose que nous devons protéger : « I have to confess that I am sympathetic to this view, and not just because it is held by many wise people judgment I trust. There's a lot of merit in the idea that privacy is an intrinsic good. » (2022, p. 67) Cependant, pour des raisons stratégiques, il propose que nous nous attardions uniquement à sa valeur instrumentale. Il fait cette proposition pour faire l'économie d'un débat potentiellement interminable sur son existence, sur sa nature ou sur sa valeur intrinsèque. En tant que défenseur de la protection de la vie privée, il lui semble plus fructueux d'aborder la question sous l'angle de l'utilité du concept de manière à convaincre les sceptiques. En effet, en considérant que la plupart des individus accordent plus de mérite à la commodité associée à l'usage du numérique ou au sentiment de sécurité

procuré par les technologies de surveillance, il paraît plus convaincant de faire référence aux valeurs que la protection de la vie privée permet de faire prospérer :

> If we want to talk about privacy with those who are unconvinced about its value, intrinsic or otherwise, I believe it's essential to talk and think about privacy as being instrumental. There is nothing inherently good or bad about information flowing or not, but as we've seen, information flows and privacy rules have consequences. Because we must inevitably craft privacy rules of one sort or another, we will need to figure out what values we want to advance and what ends we want to achieve when we regulate the collection, flow, use, storage and life cycle of human information. Because human information is everywhere, privacy discussions will frequently involve difficult trade-offs between privacy and other values. […] Specifying the values that privacy rules can serve is essential if we want to resolve those conflicts in a socially beneficial way. (2022, p. 68-69)

Il faut souligner ici que, pour Richards, la protection de la vie privée relève moins de la préservation d'une certaine dignité humaine que d'une lutte pour maintenir l'équilibre du pouvoir. En partant du principe que la détention de l'information permette d'avoir une certaine ascendance sur la nature ou sur les autres personnes — comme le rappelle l'adage bien connu, « le savoir, c'est le pouvoir » —, la protection de la vie privée consiste à faire des choix collectifs quant aux types de rapports de pouvoir que nous voulons voir exister dans notre société. Ainsi, Richards formule l'idée que la protection de la vie privée n'existe que par les règles qui visent à juguler l'asymétrie des pouvoirs entre le citoyen ou le consommateur et le gouvernement ou l'entreprise, ces derniers qui détiennent des ressources (juridiques, humaines, matérielles, financières, etc.) qui leur confèrent inévitablement un avantage informationnel sur les premiers. C'est pourquoi il conclut dans l'extrait cité qu'il importe de définir en amont quelles sont les valeurs qui doivent être promues par les mécanismes de protection qui seront mis en place. Par exemple, une société qui voudrait favoriser la sécurité publique et la cohésion sociale pourrait le faire au détriment de la liberté d'association ou de la protection des minorités en limitant fortement l'expectative de vie privée de ses citoyens et en permettant la mise en place de programme de surveillance ubiquitaire. La définition des valeurs qui guident la mise en place de ces mécanismes de protection passe par la délibération collective.

L'autonomie a été traditionnellement au cœur de ces valeurs ayant guidé la mise en place des mécanismes juridiques de protection de la vie privée, avec le consentement et l'exercice de droits individuels comme principaux leviers de mise en œuvre. Toutefois, en considérant les limites rencontrées[37] par ces leviers dans le contexte de la transformation numérique des sociétés, le fardeau de la protection de la vie privée s'est en partie déplacé vers les organisations. Les processus d'évaluation des risques et des préjudices, comme les évaluations des facteurs relatifs à la vie privée, ont ainsi été mis en place pour suppléer aux lacunes de ces leviers, et ce, en misant sur la responsabilisation et l'autorégulation des organisations. Ces processus demeurent toutefois neutres du point de vue axiologique : c'est dans l'exécution que se révéleront les valeurs mises de l'avant par l'organisation qui réalise l'évaluation.

Quelles pourraient être les différentes valeurs que les sociétés occidentales libérales et démocratiques pourraient vouloir protéger par la protection de la vie privée? Dans un rapport récent portant sur l'Internet des objets, la Commission de l'éthique en science et en technologie du Québec (CEST) a relevé cinq interprétations de ce qu'est la vie privée et des raisons qui pourraient motiver sa protection (CEST, 2020a, p. 11-12). D'abord, il y aurait les approches libérales pour lesquelles le droit à la vie privée rend possible la mise en œuvre des valeurs libérales et, de ce fait, acquiert une valeur importante pour les démocraties libérales dans lesquelles nous évoluons. La protection de la vie privée s'approcherait ainsi de la notion de « bien premier » qui est celle de John Rawls. Qu'est-ce qu'un bien premier? Pour Rawls, il s'agit d'un bien dont toute personne raisonnable voudrait pouvoir bénéficier dans une société :

> Comme première étape, supposons que la structure de base de la société répartisse certains biens premiers (primary goods), c'est-à-dire que tout homme rationnel est supposé désirer. Ces biens, normalement, sont utiles, quel que soit notre projet de vie rationnel. Pour simplifier, posons que les principaux biens premiers à la

[37] À ce sujet, voir notamment la section 1.2.2.

> disposition de la société sont les droits, les libertés et les possibilités offertes à l'individu, les revenus et la richesse. (Rawls, 2009, p. 93)

Ces biens premiers sont nécessaires à ce que Rawls nomme le projet de vie de cette personne :

> L'idée principale est que le bien d'une personne est déterminé par ce qui est, pour elle, le projet de vie à long terme le plus rationnel, à condition de se placer dans des circonstances suffisamment favorables. Un homme est heureux quand il réussit plus ou moins à réaliser ce projet. Pour le dire rapidement, le bien est la satisfaction du désir rationnel. Nous devons supposer, alors, que chaque individu a un projet rationnel de vie établi en fonction des conditions auxquelles il est soumis. Ce projet est fait pour permettre la satisfaction harmonieuse de ses intérêts. Il planifie ses activités afin que des désirs différents puissent être satisfaits sans entrave. On y parvient en rejetant les autres projets qui ont moins de chances de succès ou qui ne permettent pas une réalisation aussi complète des objectifs. (2009, p. 123)

La CEST présente ensuite les approches qui justifient la protection de la vie privée en posant qu'elle est nécessaire pour entretenir des relations personnelles et intimes, relations qui sont importantes pour l'épanouissement personnel. D'autres approches tissent des liens entre le droit à la vie privée et le droit à la propriété privée : la protection de la vie privée est nécessaire aux individus d'une façon similaire au fait que la confidentialité est nécessaire pour les entreprises privées (par exemple, pour préserver le secret industriel)[38]. D'autres approches font de la protection de la vie privée un mécanisme important pour préserver les individus de nuisance externe. Dans un tel contexte, la protection de la vie privée devient un instrument permettant de contrer divers torts.

La CEST identifie finalement les approches féministes pour lesquelles la protection de la vie privée est à la fois nécessaire pour l'exercice de certains droits par les femmes ou néfaste lorsqu'il permet de dissimuler les possibilités de domination sur celles-ci. Par exemple, la célèbre cause Roe v. Wade (410 U.S. 113) concernant le droit à l'avortement, jugement au cœur de nombreux et houleux débats publics aux États-Unis, s'articulait autour d'un argument qui fait appel au droit des femmes à la protection de leur vie privée. Bien que

[38] Solove avait lui aussi souligné que les conceptions théoriques qui font du droit à la vie privée un droit *au secret ou à la confidentialité* s'apparentent, dans les faits, aux droits économiques (voir section 2.2.2).

la Cour suprême américaine n'ait pas jugé le droit à la protection de la vie privée comme étant absolu, elle était d'avis à l'époque que l'interdiction totale de l'accès à l'avortement sécuritaire constituait une importante atteinte au droit d'une femme de disposer de son corps. Ce jugement a été tout récemment infirmé par la Cour suprême par une décision s'appuyant sur une interprétation originaliste de la Constitution américaine. Selon cette position originaliste du droit, la Constitution doit être interprétée en fonction de la signification qu'elle avait au moment de sa proclamation. Or, celle-ci ne fait pas explicitement mention d'un droit à l'avortement sécuritaire, ni d'ailleurs d'un droit à la vie privée, comme le rappelle Scott Skinner-Thompson : « Privacy is not specifically mentioned in the U.S. Constitution. But for half a century, the Supreme Court has recognized it as an outgrowth of protections for individual liberty. » (Skinner-Thompson, 2022) Cela fait craindre à plusieurs que la chute de Roe v. Wade pourrait entraîner dans son sillage nombre d'autres jugements s'appuyant sur un raisonnement similaire, notamment en matière de contraception ou de mariage entre personnes de même sexe. (Bracy, 2022; Sullivan, 2022) Cette situation est par ailleurs un très bel exemple du caractère hautement contextuel et instable de la protection de la vie privée. Elle illustre de façon malheureuse l'idée que les conditions sociales, juridiques ou politiques peuvent venir influencer drastiquement la sensibilité d'un renseignement. Le renversement de Roe v. Wade soulève en effet d'importantes préoccupations quant à l'utilisation qui pourrait être faite de certaines catégories de données par les différents États américains qui seront tentés de légiférer de façon très coercitive en matière d'avortement, notamment pour les données de géolocalisation (facilitant le repérage des personnes fréquentant une clinique d'avortement) ou celles résultant de l'utilisation d'outils de suivi de cycle menstruel ou de suivi de l'état de santé (par exemple, celles obtenues par les bracelets connectés, qui permettraient, grâce à l'intelligence artificielle, d'identifier les femmes enceintes) (AFP, 2022a, 2022b; Cox, 2022; Matsakis, 2022; Olson, 2022). Pour répondre à certaines de ces préoccupations, l'entreprise Google annonçait au moment d'écrire ces lignes qu'elle allait supprimer automatiquement les données de localisation des utilisateurs en cas de visite d'une clinique spécialisée dans les avortements pour éviter qu'elles soient utilisées par les autorités

ou par des tiers malintentionnés à l'encontre des personnes qui auraient fréquenté ces cliniques (AFP, 2022c).

La professeure de droit Julie Cohen (2013) souligne que la protection de la vie privée est essentielle pour la constitution du « soi libéral » en établissant et en préservant un espace où l'individualité, l'innovation et la créativité peuvent librement s'exprimer. Richards (2022) souligne lui aussi que la protection de la vie privée permet l'épanouissement de la personne et favorise la constitution de l'identité, mais ajoute qu'elle protège plus largement la liberté et les individus. La mise en place de mesures de protection de la vie privée aurait, selon lui, une fonction triple : permettre d'abord le développement et l'épanouissement de l'individu en tant qu'humain en ménageant un espace privé qui lui permet de former son identité personnelle; permettre le développement et l'épanouissement de l'individu en tant que citoyen en ménageant un espace où il est libre d'expérimenter les différentes idées politiques; et, finalement, protéger l'individu en tant que consommateur qui n'est pas ou qui est mal outillé et dépourvu face aux aléas de la vie informationnelle et technologique dans laquelle il évolue désormais. Moore (2003) souligne lui aussi l'importance de la protection de la vie privée pour l'épanouissement personnel, mais étend celle-ci à la préservation de la santé psychologique des individus[39]. Véliz (2020, p. 71-75) soutient que la protection de la vie privée est nécessaire pour permettre aux individus d'être véritablement autonomes et libres. Même si la protection de la vie privée peut être vue comme un frein à l'innovation parce qu'elle impose parfois des barrières aux organisations qui ne peuvent être ignorées, elle est, de l'avis des professeurs de droit Julie Cohen et Tal Zarsky, plutôt conditionnelle à l'innovation, car elle permet aux innovateurs de prendre des risques sans craindre outre mesure d'être punis ou ostracisés en cas d'erreur (Cohen, 2013; Zarsky, 2015). Plusieurs, dont Véliz, Richards, Lisa Austin et Nick Couldry et Ulysses Mejias, ne sont pas sans rappeler que la protection de la vie est d'abord et avant tout une affaire de maintien de l'équilibre des pouvoirs entre le citoyen et son gouvernement ou entre le consommateur et les entreprises privées (Austin, 2014; Couldry et Mejias, 2020; Richards, 2022; Véliz, 2020).

[39] Solove et Citron considèrent d'ailleurs le préjudice psychologique dans leur taxonomie (voir section 1.4.3).

Dans ce contexte, protéger la vie privée, c'est conserver ses chances d'exercer un certain contrôle sur sa propre vie. Il s'agit de protéger son autonomie en préservant la liberté de faire (liberté positive) et une liberté de ne pas être entravé dans son action (liberté négative), notamment par la mise en place de mécanismes prévenant l'utilisation abusive ou nuisible des renseignements personnels. Bref, il existe un nombre important de raisons qui peuvent être invoquées pour juger importante la mise en place de mesures de protection entourant la vie privée.

Pour Richards, l'avantage de considérer la protection de la vie privée du point de vue de sa valeur instrumentale n'est pas seulement stratégique, mais également méthodologique :

> Privacy is about degree of knowing and using, and as such it requires an ethical rather than a mathematical approach to the management of information flows. It is not about value of the code of human values that inform the entire enterprise. At bottom, then, privacy (and the decisions we make about it) is ultimately a series of human questions that must be informed by human values. But if the decision to protect or regulate the collection, use, or transfer of personal information is dependent on human values other than the private-ness or public-ness of a data field, we still need to figure out exactly what those values should be. (2022, p. 65)

Ainsi, pour lui, il ne s'agit plus de chercher à définir la notion de « privacy » ni de justifier la mise en place de mesures visant à la protéger parce que de sa définition découlerait sa valeur, mais plutôt de voir quels sont les avantages de la protéger en tant qu'instrument permettant de défendre d'autres valeurs. L'adoption d'un point de vue instrumental de la vie privée permet également de rendre compte des mésusages qui peuvent être faits des mécanismes de protection de la vie privée existants :

> It's also important to note that when we treat privacy as instrumental, the way we talk about privacy changes. We stop talking about creepiness, about whether we're Luddites of about whether our friend's privacy preferences are idiosyncratic. Instead, we start asking ourselves what rules about human information best promotes values we care about, what the power consequences of those rules might be, and how we should use those rules to advance the values on the ground. From this perspective, privacy becomes more neutral. This is important because privacy rules can promote bad things, too. (Richards, 2022, p. 109-110)

Parce que cette position neutralise la protection de la vie privée d'un point de vue axiologique — elle n'est plus bonne ou mauvaise en soi —, il est possible de critiquer les usages qui en sont faits. Ce sont ces usages qui deviennent bons ou mauvais. Les critiques féministes auront, à juste titre, souligné que des violences ont été perpétrées à des femmes en secret, sous le couvert de la prétendue protection de la vie privée. L'administration de la justice ou la sécurité des personnes peut parfois être compromise par des considérations de protection de la vie privée. Autrement dit, il est possible de desservir également l'actualisation de certaines valeurs en invoquant la protection de la vie privée à outrance ou à mauvais escient. Je rappelle d'ailleurs que le droit à la protection de la vie privée n'est pas considéré comme un droit absolu au Québec et au Canada :

> Toutefois, le droit à la vie privée, comme tout droit fondamental, n'est pas absolu. Il s'exerce notamment dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec. Il est donc prévu qu'on puisse y porter atteinte, en certaines circonstances et à certaines conditions, afin d'assurer un équilibre et une pondération entre les besoins de la société et les droits des individus. (CAI, 2020, p. 2)

Parce que la protection de la vie privée est une notion floue, complexe, contestable, multiple, mais qu'elle permet tout de même de protéger d'autres valeurs qui sont importantes aux yeux des sociétés libérales occidentales, il paraît tout à fait acceptable d'adopter une position similaire à celle de Richards pour parler de risque porté à la protection de la vie privée. D'ailleurs, Solove souligne lui aussi que les règles mises en place par les sociétés occidentales pour protéger la vie privée l'ont été justement parce que celles-ci ont trouvé profitable de le faire :

> […] when privacy protects the individual, it does so because it is in society's interest. Individual liberties should be justified in terms of their social contribution. Privacy is not just freedom from social control but is in fact a socially constructed form of protection. The value of privacy does not emerge from each form of privacy itself but from a range of activities it protects. (2008, p. 173-174)

Ce constat de Solove s'appuie sur une simple observation empirique : les législateurs et les juristes ont jugé bon d'établir des lois pour encadrer la protection de la vie privée et de sévir

lorsque celles-ci ne sont pas respectées. La recension de ces lois et de ces jugements est d'ailleurs, je l'ai mentionné, à la source même de son travail de taxonomiste des activités susceptibles de porter atteinte à la vie privée et des préjudices portés à celle-ci (voir section 1.4.3).

Cette prise de position n'est pas sans conséquence pour la réalisation des ÉFVP. Si ceux qui réalisent un processus des risques veulent pouvoir prétendre protéger effectivement ce qui est visé par la notion de vie privée, elle ne doit pas se limiter uniquement à envisager les risques associés traditionnellement à la protection des renseignements personnels, ni même à la protection de la vie privée, mais doit envisager plus largement tous les risques associés plus traditionnellement aux évaluations proprement éthiques. Elle devrait tenir compte des impacts plus larges que le projet pourrait engendrer sur la société, sur les populations vulnérables, sur les droits de la personne, etc. C'est d'ailleurs l'une des particularités de l'analyse d'impact à la protection des données prévues au *Règlement général sur la protection des données* (RGPD) qui, contrairement à la loi québécoise, stipule explicitement que le risque évalué doit être celui qui concerne les droits et libertés des personnes physiques[40].

[40] L'article 35 du RGPD précise de manière explicite cette emphase sur les droits humains : « 1. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. […] 7. L'analyse contient au moins : […] a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. »

À ce titre, voir également les considérants 74 à 78

2.4.2 Le lien entre la PRP et la protection de la vie privée informationnelle

La protection des renseignements personnels est la matérialisation juridique de la protection de la vie privée informationnelle. Elle est donc subsumée à la notion plus large de protection de la vie privée et, de ce fait, elle partage des caractéristiques communes avec celle-ci qu'il paraît important de rappeler.

D'abord, comme le souligne Solove, la protection de la vie privée peut être conceptualisée comme étant la possibilité d'exercer un *contrôle sur ses renseignements personnels* (« *Control over Personal Information* »). Cette conception s'articule autour de l'idée que le renseignement personnel est une extension de la personne et que, de ce fait, il doit être protégé d'une façon analogue. Or comme le démontre la pluralité des conceptions théoriques, protéger la vie privée ne se limite pas uniquement au fait pour une personne de contrôler et de gérer l'accès à ses renseignements personnels ni au fait qu'un tiers les sécurisent une fois qu'ils sont collectés. Nous savons également que la protection de la vie privée informationnelle est une dimension particulière de la vie privée qui surplombe et recoupe toutes les autres dimensions de cette dernière (Koops & coll., 2017). Elle est en quelque sorte une *métadimension* de la vie privée. La protection de la vie privée informationnelle n'est pas garantie du seul fait de protéger la confidentialité d'un renseignement ou d'une donnée : elle s'actualise, par extension, dans le fait de protéger les autres dimensions de la vie privée de la personne concernée par ce renseignement ou cette donnée. De mon point de vue, prétendre protéger la vie privée en ne s'attardant qu'à la PRP — c'est-à-dire uniquement à la dimension informationnelle de la protection de la vie privée — est réducteur : la protection de la vie privée ne s'épuise pas dans la protection des renseignements personnels et, encore moins, dans les seuls mécanismes mis en place pour garantir la sécurité de l'information et la cybersécurité.

Nous savons aussi que les attentes en matière de protection de la vie privée informationnelle sont des normes fortement influencées par le contexte dans lequel elles se matérialisent. Comme le rappelle Nissenbaum (2009), l'individu ne perçoit pas d'atteinte à

sa vie privée si ses renseignements personnels circulent de façon conforme à ses attentes, si ce flux informationnel est conforme à ce qu'elle nomme l*'intégrité contextuelle*. De ce fait, on peut s'attendre à ce que l'application des mécanismes de protection des renseignements personnels tienne compte du contexte. Finalement, nous avons vu avec Richards qu'il était stratégiquement plus fructueux d'aborder la protection de la vie privée en la considérant comme instrument en vue de préserver autre chose (comme la liberté, l'autonomie, la démocratie, les relations interpersonnelles, etc.) plutôt que de s'entêter à lui prêter une valeur intrinsèque. Ainsi, il paraît tout autant judicieux d'envisager la protection des renseignements personnels sous l'angle de l'instrument. Comme le fait remarquer Solove :

> Since privacy is a pluralistic concept, its value should be understood pluralistically as Well. Privacy does not have a uniform value. Its value varies across different contexts depending upon which form of privacy is involved and what range of activities are imperiled by a particular problem. (2008, p. 173)

Il paraît d'autant plus pertinent de prendre une telle position considérant que, en tant que matérialisation juridique de la protection de la vie privée informationnelle, elle recoupe toutes les autres dimensions de la protection de la vie privée au même titre que la protection de la vie privée. Parce qu'elle surplombe et touche toutes les autres dimensions de la protection de la vie privée, la protection des renseignements personnels est *déjà* un instrument en vue de protéger : en protégeant le renseignement, elle protège également les autres dimensions de la vie privée identifiées par Koops *et al.* En protégeant les renseignements personnels, nous concourrons tout autant à protéger *la vie privée corporelle, intellectuelle, spatiale, décisionnelle, communicationnelle, associative, possessionnelle* et *comportementale* (voir section 2.3). Cette action transitive de la protection des renseignements personnels doit se refléter dans les évaluations des risques : le risque qui doit être évalué ne devrait pas être celui qui concerne le renseignement en lui-même, mais bien le sujet de ce renseignement, en considérant que l'objet de ce risque (la vie privée) est multidimensionnel (2.3.1), contextuel et centré sur la perception individuelle (2.3.2) et, dans certains, cas, inconnu et prospectif (2.3.3).

2.5 *CONCLUSION*

Sans prétendre avoir été exhaustif dans ma démarche, le tour d'horizon succinct et forcément incomplet que j'ai proposé permet de voir que la notion de protection de la vie privée bénéficie d'une pluralité de définitions et, surtout, qu'elle est très complexe. La réponse à la question « qu'est-ce que "protéger la vie privée"? » n'est pas unique : elle est multiple. La coexistence de multiples définitions est, de l'avis de Mulligan, Koopman et Doty (2016), l'une de ses composantes essentielles en tant qu'objet de connaissance. Et plus encore que la multiplicité des réponses que l'on peut donner à la question du sens et à celle de l'étendue de la notion de « protection de la vie privée », les faits qu'elle demeure contestable dans son essence et qu'elle pourrait, dans l'absolu, n'être rien en soi militent en faveur d'un changement de stratégie pour celui qui entend la défendre. S'il s'avère hasardeux de s'appuyer sur une quelconque « essence » de la protection de la vie privée pour prétendre la défendre, il l'est probablement tout autant de vouloir définir la notion de « risque porté à la vie privée » en ne s'attardant qu'à l'une ou l'autre de ses composantes ou en s'appuyant sur une définition qui s'avère *essentiellement* incomplète et fluctuante. Dans ce contexte, la protection de la vie privée *informationnelle* n'est qu'une de ses différentes dimensions. Dire que l'on protège la vie privée *dans son ensemble* en se limitant à cette seule dimension ne paraît pas juste. Bien qu'il serait incorrect de dire que la considération des risques et des préjudices portés à la protection des renseignements personnels dans le cadre d'une ÉFVP ne soit pas utile, il serait simplement erroné de dire que la vie privée est protégée parce que les renseignements personnels ou les données le sont. Toute action entreprise pour défendre les renseignements personnels concourt à augmenter le niveau général de protection de la vie privée.

Je pose l'hypothèse suivante : les évaluations des risques et des préjudices portés à la vie privée doivent correspondre à une évaluation plus générale des risques éthiques pour prétendre atteindre leur objectif, et ce, afin de rendre compte de la complexité de ce que veut dire « protéger la vie privée ». D'ailleurs, l'évaluation des risques aux droits de la personne est déjà au cœur de l'obligation de réaliser des *analyses d'impact à la protection des données*

en droit européen, et la Commission des droits de la personne et de la protection de la jeunesse faisait la recommandation de remplacer l'ÉFVP par une évaluation des facteurs relatifs aux droits et libertés de la personne garantis par la Charte lors des auditions et consultations particulières sur le projet de loi 64 (CDPDJ, 2020). Toutefois, le fait d'élargir l'évaluation des risques et des préjudices portés à la vie privée aux risques éthiques vient complexifier davantage cette opération qui, indépendamment de cet ajout, requiert déjà des compétences juridiques et technologiques importantes. Ainsi, les constats qui ont été faits dans ce chapitre et dans le premier me permettront d'aborder certains enjeux éthiques des évaluations des risques et des préjudices portés à la vie privée.

CHAPITRE 3
QUELQUES ENJEUX ÉTHIQUES CONCERNANT L'ÉVALUATION DES RISQUES ET DES PRÉJUDICES PORTÉS À LA VIE PRIVÉE

3.1 *INTRODUCTION*

Les deux premiers chapitres de ce mémoire ont été réalisés dans l'objectif de mettre en lumière la complexité de la composante « gestion des risques et des préjudices portés à la vie privée » des évaluations des facteurs relatifs à la vie privée (ÉFVP). J'ai d'abord mis en lumière le concept d'ÉFVP et posé les grandes lignes des processus d'évaluation des risques et des préjudices en général dans le but d'établir une compréhension commune de ces processus. J'ai surtout voulu exposer le fait que les risques et les préjudices portés à la vie privée débordent des obligations mises en place par les lois de protection des renseignements personnels. Ils vont au-delà des considérations juridiques et des considérations de sécurité de l'information ou de cybersécurité. Ils s'étendent, comme Daniel Solove, Danielle Keats Citron et d'autres l'ont proposé, aux dimensions physique, économique, réputationnelle, relationnelle et psychologique de la vie des personnes concernées par l'information colligée, utilisée ou communiquée dans le cadre d'un projet. Comme souligné à la section 1.4.3, les risques portés à la vie privée peuvent entraîner des préjudices de diverses natures. Par exemple, ils peuvent engendrer une atteinte à l'autonomie et à la liberté des personnes, peuvent produire des effets discriminatoires ou engendrer une détresse émotionnelle auprès des personnes qui les subissent.

Mon second chapitre poursuivait dans cette direction. Mon objectif a été de présenter les difficultés rencontrées par les théoriciennes et théoriciens qui tentent de répondre à la question « qu'est-ce que "protéger la vie privée"? » et de montrer la multiplicité des réponses potentielles. Ce fut l'occasion de mentionner au passage l'hypothèse de Deidre Mulligan, Colin Koopman et Nick Doty que cette question pourrait ne jamais pouvoir obtenir de réponse définitive. Pour toutes ces raisons, il semble qu'un processus d'évaluation des risques et des préjudices portés à la vie privée s'apparente davantage aux processus plus

généraux d'évaluation des risques éthiques, comme ceux prévus par exemple dans les processus d'évaluation des projets de recherche avec des humains (Gouvernement du Canada, 2018).

Ce troisième et dernier chapitre vise à esquisser quelques implications éthiques pour la réalisation des ÉFVP. Ces implications découlent des constats faits dans le premier et second chapitre. Dans la première section, je cherche à montrer que les caractéristiques des risques et des préjudices portés à la vie privée diminuent les chances que ces derniers soient estimés à la hauteur de la considération portée à la protection de la vie privée dans nos sociétés libérales et démocratiques occidentales. Parce que ces risques engendrent, dans une grande proportion, des impacts mineurs ou imperceptibles, il est probable qu'ils soient jugés peu importants lorsqu'ils seront mis en opposition à la commodité promise aux citoyens ou aux consommateurs par la mise en place d'un système d'information ou d'une prestation électronique de service ou comparés à l'avantage compétitif ou stratégique convoité par l'organisation. En outre, certains des risques et des préjudices portés à la vie privée ne visent pas des individus spécifiques, mais concernent plutôt des populations ou des sous-groupes, notamment des groupes de personnes plus vulnérables. Étant donné que les lois de protection de renseignements personnels mettent l'individu au centre des préoccupations, ces risques collectifs pourraient tout simplement ne pas être considérés dans le processus d'évaluation. Pour finir, il va s'agir de renforcer l'idée avancée au second chapitre que les risques et les préjudices portés à la vie privée existent surtout dans l'œil de la personne qui les subit. Cette réalité implique que le processus d'évaluation devrait prévoir des mécanismes permettant d'intégrer le point de vue des personnes concernées, faute de quoi il risque de s'avérer partiel et partial.

La seconde section concerne davantage la personne de l'évaluateur même. Il s'agit d'abord de mettre en relief les présupposés utilitaristes qui sous-tendent les processus d'évaluation en général. Ces processus relèvent d'une perspective utilitariste du fait qu'ils visent à établir un rapport entre les bénéfices escomptés par un projet et les préjudices potentiels qu'il engendre. Considérant que l'arbitrage entre les bénéfices et les préjudices

repose en partie sur les inclinaisons personnelles et les compétences de l'évaluateur, ainsi que sur les objectifs poursuivis par l'organisation, notamment au moment d'établir le domaine d'application du processus d'évaluation, il existe des risques de conflits d'intérêts dans la réalisation d'un processus. Ces derniers peuvent mener à remettre en question l'objectivité de la démarche. En outre, la réalisation d'une telle évaluation exigerait probablement l'adoption d'une certaine posture professionnelle qui impliquerait notamment d'avoir la sécurité du public au centre des préoccupations. Finalement, il s'agira de souligner certaines données qui permettent de mettre en doute la faisabilité de l'obligation légale de réaliser des ÉFVP pour l'ensemble des projets impliquant un système d'information ou une prestation électronique.

Je ne prétends pas devoir traiter exhaustivement de ces différents enjeux dans ce troisième chapitre. Considérant les limites d'un mémoire de maîtrise, il s'agit surtout d'en dresser les grandes lignes. Je ne prétends pas non plus avoir exploré tous les enjeux potentiels liés à cette nouvelle obligation. Il s'agit simplement de mettre en relief certaines problématiques qui pourront faire l'objet d'un approfondissement ultérieurement. En outre, il ne faut pas perdre de vue que l'obligation de réaliser de telles évaluations n'a pas encore été mise à l'épreuve de la réalité : elle ne le sera qu'à partir de septembre 2023. Ainsi, ces considérations sont soulevées dans une perspective prospective, et la pratique et le temps pourront venir corroborer ou infirmer les appréhensions que je soulève.

3.2 *LA PROTECTION DE LA VIE PRIVÉE DANS LE CONTEXTE D'UNE ÉVALUATION D'UN PROJET INFORMATIQUE*

3.2.1 Les caractéristiques des risques et des préjudices portés à la vie privée confrontées à l'évaluation

On retrouve dans la section 1.4.3 deux taxonomies portant sur des aspects différents de la protection de la vie privée. La première taxonomie élaborée par Daniel Solove expose certaines activités qui donnent lieu potentiellement à des atteintes à la vie privée. La seconde, celle-là produite en collaboration avec Danielle Keats Citron, concerne plus spécifiquement

les préjudices à la vie privée qui peuvent être engendrés par les activités mises en lumière dans la première taxonomie. Ces deux taxonomies représentent des sources de scénarios de risques que les organisations pourraient utiliser pour réaliser une ÉFVP. Toutefois, sans remettre ni leur qualité ni leur pertinence en question, ces deux taxonomies apparaissent incomplètes. Elles peuvent l'être d'abord parce qu'elles s'appuient sur une analyse de la jurisprudence américaine. Elles ne traitent que des activités ou de préjudices qui ont été reconnus ou abordés par les cours de justice américaines. Comme James Whitman le souligne, le droit à la vie privée est érigé sur des principes différents de part et d'autre de l'Atlantique. Alors que c'est la protection de la dignité de la personne qui sous-tend le droit européen, c'est plutôt celui du maintien de la liberté individuelle qui aurait animé le droit américain, menant d'une part à un droit de la protection de la vie privée axé sur les droits de la personne et de l'autre, sur la préservation de la liberté de la personne, notamment à l'égard du pouvoir gouvernemental (Whitman, 2004). Il est ainsi probable que l'analyse de la jurisprudence d'autres législations aurait soulevé des préjudices différents. En outre, ces taxonomies peuvent être incomplètes en raison des caractéristiques de la vie privée soulevées tout au long du second chapitre. Comme le souligne Helen Nissenbaum, la caractérisation de ce qui constitue une atteinte à la vie privée est profondément reliée au contexte. Également, suivant le raisonnement de Mulligan, Koopman et Doty, le concept même de « vie privée » peut être *essentiellement contestable*, c'est-à-dire qu'il pourra faire l'objet d'une reconfiguration sempiternelle de ses constituantes conceptuelles internes en raison de l'évolution du contexte à partir duquel il se définit. Autrement dit, toute taxonomie est forcément vouée à évoluer avec le contexte, notamment avec le contexte technologique. Solove est d'ailleurs conscient des limites de sa méthode (2008, p. 196-97). Mais par-delà ces considérations méthodologiques et conceptuelles, Solove et Citron (2021) soulèvent eux-mêmes trois difficultés pratiques rencontrées par les juristes et législateurs lorsqu'ils abordent la question des préjudices portés à la vie privée. Ces remarques concernent : la gravité des préjudices, l'intervalle qui peut exister entre la matérialisation de l'événement et le préjudice qu'il cause et, finalement, la nature sociétale de certains risques.

D'abord, comme Solove le fait remarquer dans un autre texte que *Understanding Privacy*, « [m]ost privacy problems lack dead bodies » (2007, p. 768). Sans dire qu'il n'existe aucun exemple spectaculaire d'atteintes et de torts causés à la protection de la vie privée[41], ses défenseurs souffrent d'un manque d'exemples qui frappent l'imaginaire. De ce fait, poursuivent Solove et Keats Citron, « [a] major complicating dimension of many privacy harms is that they are small but numerous » (2021, p. 816). Ils soulignent ainsi que les torts ou les préjudices qui sont causés effectivement à la protection de la vie privée sont souvent plutôt insignifiants lorsqu'ils sont considérés à l'unité. Malgré cette apparente bénignité, ils touchent parfois un nombre impressionnant de personnes ou ils atteignent un même groupe de personnes à plusieurs reprises. À titre d'exemple, la réception d'un courriel indésirable constitue en soi une intrusion. Elle engendre une atteinte — petite, convenons-en — à la quiétude d'une personne. La plupart du temps, ce courriel intempestif est rapidement effacé et son destinataire passe à autre chose. Mais le dérangement s'additionne du fait d'en recevoir deux ou trois par jour, sur trois cent soixante-cinq jours par année. Il faut, en plus, considérer que ces courriels indésirables représentent autant de petits bris potentiels de la concentration causés par la notification qui l'accompagne. Il faut tenir compte de la perte de temps passé à les gérer, même si cela peut ne prendre que quelques secondes à la fois. Il faut envisager la possibilité que chacun de ces courriels dissimule une tentative d'hameçonnage ou qu'il recèle un virus ou un rançongiciel, menant potentiellement à des préjudices plus sérieux pour la personne qui le reçoit[42]. Bien sûr, il existe des outils technologiques permettant de gérer l'afflux de courriels indésirables, mais l'usage de ces derniers engendre lui aussi de légers désagréments, comme celui de ne pas prendre connaissance d'un message important au bon

[41] Évoqués à la section 2.4.1, l'histoire de l'utilisation des données du recensement néerlandais par les nazis et les effets potentiels de la remise en cause de Roe v. Wade aux États-Unis sont des exemples de problèmes plus spectaculaires en matière de protection de la vie privée, comme le sont également le vol important de données chez Desjardins et l'affaire Cambridge Analytica sur lesquels je reviens dans les prochaines pages. Toutefois, comme Solove le souligne, « [t]here is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized » (2007, p. 768).

[42] Même si cette considération n'est pas liée à la protection de la vie privée, j'ajouterais que le coût environnemental des courriels indésirables n'est pas négligeable considérant la quantité importante d'électricité nécessaire à la transmission et à la conservation des courriels (FCC, 2022; McAfee, 2009).

moment parce que ce dernier est tombé dans la boîte de courriels indésirables. Dans un registre plus grave, les interpellations policières (qui peuvent être tout à fait légitimes à la base et peu intrusives selon le contexte [par exemple, dans le cadre d'une opération spéciale]) touchent généralement un nombre moins important d'individus. Toutefois, lorsqu'elles touchent une même catégorie de personne de manière disproportionnée, il peut être question de profilage ethnique. C'est donc l'addition de ces petites atteintes qui pourrait constituer, collectivement, un problème majeur porté à la vie privée. Or, ces problèmes échappent en grande partie au contrôle des entreprises et des organismes publics. D'une certaine façon, la loi tolère ces *micropréjudices*, car elle ne sait pas trop comment les gérer : « The result makes privacy violations large-scale problems that cause a significant societal impact, but that do not fit readily into the traditional way the law looks at harm. » (Solove et Keats Citron, 2021, p. 19)

Dans le cadre d'un processus d'évaluation des risques et des préjudices, l'impact de tels micropréjudices serait probablement trop négligeable pour être considéré par l'évaluateur. En fait, les risques identifiés pour ces micropréjudices pourront tomber sous la limite de la préoccupation (voir page 133). Dans une grande majorité des cas, le risque donnant lieu à un tel micropréjudice pour un individu donné serait probablement écarté d'emblée, car jugé non pertinent ou ayant trop peu d'impact. S'il advenait qu'il soit considéré malgré tout, il souffrirait probablement d'un déficit d'importance face aux bénéfices escomptés par la mise en place d'une solution technologique. Et cela ne paraît pas surprenant : l'adhésion massive aux technologies de l'information permet de penser que les citoyens et les consommateurs en arrivent généralement au même résultat lorsque vient le temps d'évaluer leur propre rapport coût-bénéfice. Autrement dit, en consentant à la collecte et à l'utilisation de renseignements personnels en échange d'un service ou d'un bien, il paraît légitime de présumer que la personne concernée a fait elle aussi une certaine évaluation de

ses propres risques, jugeant ceux-ci généralement assez négligeables[43] (ce qui sous-entend qu'elle a été préalablement informée des risques pour donner un consentement valable).

Il devient plus difficile d'évaluer un seuil critique de gravité ou de probabilité pour la somme de ces micropréjudices. C'est-à-dire : à quel moment cette somme devient-elle suffisamment préjudiciable pour devenir un enjeu? Il est également pensable que le principe de précaution soit rarement invoqué pour gérer de tels risques. Pour la Commission mondiale d'éthique des connaissances scientifiques et des technologies (COMEST), le danger moralement inacceptable serait celui qui est «

- menaçant pour la vie ou la santé humaine, ou bien
- grave et réellement irréversible, ou bien
- inéquitable pour les générations présentes ou futures, ou bien
- imposé sans qu'aient été pris dûment en compte les droits humains de ceux qui le subissent » (COMEST, 2005, p. 14).

Considérant que les micropréjudices portés à la vie privée seront rarement « menaçants pour la vie ou la santé humaine », « graves et réellement irréversibles » ou « inéquitables pour les générations présentes ou futures », ils risquent de n'apparaître nulle part. Le dernier critère, soit celui d'être « imposé sans qu'aient été pris dûment en compte les droits humains de ceux qui le subissent », paraît mal adapté à ces petits préjudices, parce que l'impact sur les droits humains pourrait très bien avoir été pris en compte dans l'évaluation du préjudice « à l'unité », sans toutefois que les impacts de l'addition ou de l'accumulation de ceux-ci aient été considérés par l'évaluateur.

Solove et Keats Citron soulignent également qu'un tort ou un préjudice à la vie privée n'est pas nécessairement ressenti par la ou les personnes impliquées. Par exemple, une fuite de données n'est pas douloureuse en soi, même s'il s'agit d'un préjudice et d'une atteinte à

[43] Je pourrais bien sûr remettre en question la pertinence du consentement dans le contexte d'un projet gouvernemental. Il est toujours plus difficile de s'extraire d'une obligation gouvernementale.

la vie privée. Elle peut très bien passer inaperçue si l'événement n'est pas déclaré à la personne impliquée dans celle-ci. Ou bien, les personnes qui sont victimes de cette fuite de données peuvent parfois en subir les contrecoups seulement après un délai important. Ces deux circonstances — l'absence de ressenti ou le délai avant le ressenti — peuvent diluer la perception du lien de cause à effet entre l'événement et le préjudice qui en découle. Solove et Keats Citron ajoutent que « [p]rivacy harms often not only involve a future risk of injury, but they are compounded by an additional dimension of complexity: the range of possible future injuries is much more varied » (2021, p. 21). C'est dire en fait que, en plus du délai encouru potentiellement entre l'événement initial et le préjudice (ou avec le ressenti du préjudice), d'autres événements peuvent advenir et s'ajouter dans la chaîne de causalité. Nous pouvons penser ici aux événements qui ont touché les clients de la coopérative Desjardins au Québec. Rappelons les faits : les données personnelles de 9,7 millions de clients actifs ou d'anciens clients de la Fédération des caisses Desjardins du Québec auraient été exportées des bases de données de la compagnie et dérobées par un employé pour être ensuite revendues (Chassigneux, 2020). Bien que certains des individus impliqués ont déjà subi des vols d'identité ou des fraudes depuis la diffusion des données, celles-ci circulent toujours sur Internet. Ainsi, un vol d'identité qui aurait lieu dans cinq ans pourra être, en réalité, directement lié à l'incident Desjardins, mais le lien de causalité se diluera dans le flou de la vie numérique et s'en trouvera impossible à établir. En outre, ce vol d'identité à retardement pourrait également impliquer l'usage d'autres données obtenues ultérieurement par d'autres moyens ou d'autres sources, et ce, légalement ou non (par exemple, par le biais des réseaux sociaux ou d'une autre fuite de renseignements personnels). Ces informations supplémentaires acquises par la suite viendront brouiller les pistes. Également, l'addition d'événements — qui pourraient ne pas avoir eu lieu si la chaîne de causalité n'avait pas été mise en branle lors du premier événement — peut aggraver les impacts du risque qui, initialement, n'étaient pas si grands. Pour reprendre l'exemple de Desjardins : aux renseignements diffusés initialement peuvent s'additionner des renseignements plus sensibles encore, ouvrant ainsi la porte à des atteintes plus grande à la vie privée que ceux rendus possibles par la brèche initiale. Par exemple, les données obtenues avec l'histoire de

Desjardins pourraient un jour donner un accès indu à des données de santé ou à des données biométriques, ce qui aurait pour effet de rendre d'autant plus vulnérable la personne concernée.

Deux considérations découlent de ce délai entre le préjudice et son ressenti ou de l'absence de ressenti. Il faut d'abord souligner que les événements impondérables ne sont généralement pas considérés dans les processus d'évaluation de risque : « Le risque doit être distingué de l'incertitude, qui se rapporte à un événement dont la probabilité n'est pas mesurable et qui, par conséquent, est imprévisible. » (OQLF, 2020c) Le risque qui sera évalué doit *vraisemblablement pouvoir advenir*. L'Énoncé de politique des trois conseils sur l'éthique de la recherche avec des êtres humains ne dit pas autre chose. Même dans le contexte d'une évaluation éthique produit par un comité d'éthique de la recherche, la notion de probabilité renvoie à l'idée que [l'italique est de moi] « des participants [à la recherche] subissent *véritablement* les préjudices en question. » (Gouvernement du Canada, 2018, p. 22) Or, comme le souligne Nissenbaum, la perception des individus subissant un incident impliquant l'utilisation des renseignements personnels compte pour beaucoup dans la constitution et la perception d'une atteinte à la vie privée. Autrement dit, l'atteinte à la vie privée existe en grande partie dans le ressenti de la personne qui la subit. Il paraît improbable de penser qu'un évaluateur puisse être en mesure de considérer l'ensemble — sans doute infini — des configurations potentielles des événements engendrant une atteinte perçue à la vie privée. Et finalement, il devient rapidement impossible d'attribuer une quelconque responsabilité lorsqu'il y a accumulation de micropréjudices. Pour reprendre l'exemple des courriels indésirables, à quel moment peut-on considérer que la quantité de courriel indésirable devient véritablement préjudiciable? Qui envoie le courriel *de trop* (si une telle chose peut exister)? Considérant que de tels courriels indésirables peuvent désormais être transmis automatiquement par des logiciels — des robots ou des « bots » — l'attribution de la responsabilité individuelle de cette somme de micropréjudices peut paraître d'autant plus difficile à établir.

Il devient ainsi hasardeux d'évaluer avec justesse les impacts de tous ces risques liés à l'utilisation de renseignements personnels. En outre, l'augmentation globale et constante de la quantité de données diversifiées portant sur un grand nombre de personnes exacerbe les possibilités que des préjudices plus importants se matérialisent. Malgré tout, au moment de réaliser l'évaluation, une organisation ne trouverait que peu de leviers, sinon aucun, pour réduire les impacts additionnés de tels risques hypothétiques. Elle n'exerce probablement aucun véritable contrôle sur ces risques composés, si ce n'est celui de laisser tomber tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels. Il semble peu probable qu'il en ira ainsi dans une très grande proportion des cas.

Ainsi, si l'on prend le point de vue d'un évaluateur dans un processus d'évaluation appuyé sur une logique utilitariste[44], il semble plausible d'envisager que la plus grande partie des risques et des préjudices portés à la vie privée seront écartés d'emblée. Il semblerait même raisonnable d'agir ainsi, car les risques et les préjudices portés à la vie privée paraissent assez mineurs dans une grande majorité des cas. Généralement, la perception de l'utilité engendrée par la mise en place des projets informatiques est telle que la perspective de subir la plupart des préjudices à sa vie privée paraîtra négligeable en contrepartie. Comme le mentionnent Koivisto et Douglas :

> Expected utility is a more promising response to uncertainty. This form of consequentialism considers the probable consequences of an action. An action with a high probability of moderately good consequences would be a better choice than an action with a small chance of extremely good consequences. Similarly, actions with a significant chance of causing harmful consequences (such as running red lights while driving) would be rejected. (2015, p. 7)

Pourtant, collectivement, dans nos sociétés occidentales, nous accordons volontiers une valeur suffisante à la vie privée pour considérer qu'il est important de la protéger et pour inscrire dans les tables de lois des mécanismes de protection de la vie privée et de protection

[44] Je reviens de manière plus détaillée sur ce point à la section 3.3.1.

de renseignements personnels. Face à cette faiblesse apparente des risques et des préjudices portés à la vie privée, il subsiste quand même au Québec cette idée que la vie privée — ce bien premier au sens rawlsien — doit être protégée.

3.2.2 Les risques et les préjudices portés à la vie privée collective

Un dernier constat s'impose quant à la nature de certains risques portés à la vie privée. Solove et Keats Citron constatent que certains préjudices ne portent pas sur l'individu, mais atteignent plutôt des collectivités : « Privacy harms often involve injury not just to individuals but to society », ce qui fait que « [t]hese considerations are often omitted from the law's evaluation of harm because they do not fit the individualistic focus that courts have for cognizable harm. » (2021, p. 21) Ainsi, certains risques et préjudices encourus collectivement échapperaient aux couvertures juridiques, parce que celles-ci sont centrées autour de l'individu et construites sur la notion d'autonomie et sur le consentement individuel ou sur l'idée que le renseignement personnel est un bien dont on peut disposer selon son bon vouloir.

Tout au long des premier et second chapitres de ce mémoire, j'ai tenté de montrer que la protection de la vie privée représente une muraille pour protéger les individus de risques. Les théoriciens en matière de droit à la vie privée commencent désormais à parler de la *protection de la vie privée des groupes* (« group privacy »). Ils avancent en effet l'idée que les regroupements d'individus devraient également avoir un droit à la vie privée qui ne se résume pas à la somme des droits individuels des personnes qui les constituent (Floridi, 2017; Loi et Christen, 2020; Perron, 2020; Taylor et Floridi, 2017). C'est dire qu'il ne suffirait plus nécessairement de dire « j'ai des droits » et « tu as des droits » pour considérer que notre vie privée est protégée, mais bien de dire que le « nous » (constitué de toi et de moi) a des droits. Pour Michele Loi et Markus Christen, la notion de « groupe » peut faire référence à deux catégories de regroupement d'individus :

> Groups consisting of natural persons with an interaction history and/or collective goals in the sense of displaying some meaningful form of agency, as a group, e.g.,

> through intentional coordination, or at least awareness of themselves as a group, with which they identify. (Type-a groups.)
>
> Groups consisting of natural persons with one or more features in common, who do not have the property in (a) setting aside the trivial case of shared goals, which are pursued without a common plan, or for the common good; e.g., smokers share the goal to smoke. (Type-b groups.) (Loi et Christen, 2020, p. 2)

Simon Perron va plutôt parler de groupe « actif » et de groupe « passif » :

> Le groupe actif est composé d'individus qui sont conscients de leur appartenance au groupe et qui s'y identifient. […] Inversement, les membres d'un groupe passif ne sont pas nécessairement conscients de leur appartenance au groupe, car l'existence du groupe dépend de l'externe; c'est le regard des autres qui lui donne naissance. (2020, p. 39)

Il est aisé de trouver des exemples de groupes associés au type A : les membres d'un fan-club, les étudiants de la maîtrise en éthique à l'UQAR, les employés de telle ou telle entreprise, etc. Les groupes du second type sont constitués d'individus partageant une ou plusieurs caractéristiques. Ces derniers ne sont cependant pas nécessairement conscients de faire partie d'un groupe pour cette raison spécifique ou bien le fait d'appartenir à ce groupe ne revêt pas d'intérêt particulier à leurs yeux. Prenons les exemples suivants : les personnes ayant consulté une fiche-produit sur un site transactionnel en ligne; les élèves qu'un algorithme a étiquetés, à leur insu, comme potentiels décrocheurs; les candidats à un poste considérés à haut potentiel en raison de leurs résultats à un test psychométrique; etc. Le fait d'envisager d'étendre une certaine forme de droit à la vie privée aux groupes, notamment pour la question du profilage, acquiert une pertinence toute particulière à l'ère des technologies de l'information, et particulièrement pour les groupes de type B ou les groupes « passifs ». En effet, à l'aide de la puissance de calcul des ordinateurs d'aujourd'hui, un algorithme d'intelligence artificielle peut identifier plus facilement des motifs dans les jeux de mégadonnées menant à l'étiquetage des personnes, ce que les systèmes antérieurs ne permettaient pas de faire avec autant de facilité. Si cette capacité de traitement des données permet d'envisager des avancées importantes en matière, par exemple, de diagnostic médical par la reconnaissance de symptômes précoces de maladies, elle a déjà été utilisée pour faire

du ciblage publicitaire en ligne. À l'aide de ces capacités de générer des regroupements de personnes partageant certaines affinités, les publicitaires ont pu cibler des publics pour vendre plus efficacement leurs produits. Toutefois, ces capacités ont aussi donné lieu à des situations plus troublantes, comme l'histoire fréquemment rappelée d'une jeune fille du secondaire dont la grossesse fut révélée à son père en raison de l'envoi de bons de réduction sur des produits de bébé par la compagnie Target (Déziel, 2018, p. 832-833; Duhigg, 2012). Dans certains cas, elles ont également permis d'identifier des personnes issues de minorités vulnérables, et ce, même si ces personnes cachaient d'emblée l'information en question (Armus, 2017; Malboeuf, 2022). Dans ces deux contextes, le fait de révéler de l'information générée à partir d'autres données a privé ces personnes de leur autodétermination informationnelle. Elles n'ont pu décider elles-mêmes de révéler ou de communiquer à autrui une information — dans ces cas-ci, très sensible et très personnelle — les concernant. Ce qu'il faut retenir de cette possibilité d'étendre le droit à la vie privée aux groupes d'individus, c'est le fait que si la protection de la vie privée permet de défendre les individus, elle dessert également les collectivités et la société dans son ensemble.

Ces constatations me rapportent à l'aspect instrumental de la protection de la vie privée que j'ai soulevée à la section 2.4. Au-delà de l'évaluation des risques et des préjudices portés aux individus et ceux portés aux regroupements d'individus, l'évaluation des risques et des préjudices devrait sans doute considérer également les risques et les préjudices portés aux collectivités, au moins pour les projets de très grande envergure, comme les projets gouvernementaux susceptibles de toucher à l'ensemble de la société. La polarisation des opinions par l'usage des données est un exemple patent de préjudice causé aux collectivités. Pensons notamment à l'affaire Cambridge Analytica évoquée au premier chapitre. Serait-il pertinent pour une organisation de devoir tenir compte des risques immatériels, sociétaux ou associés à la protection de la vie privée des groupes dans les processus d'évaluation visant des situations impliquant l'acquisition, le développement et la refonte de systèmes d'information ou de prestations électroniques de services impliquant des renseignements personnels? Je m'en tiendrais à émettre une réponse brève et forcément incomplète. Encore une fois, il paraît plutôt improbable qu'une organisation considère ces risques dans ses

processus d'évaluation. Devant ces préjudices hautement hypothétiques ou difficilement mesurables, elle trouverait encore ici très peu de leviers d'intervention, si ce n'est celui de ne pas mettre en œuvre de projets impliquant des renseignements personnels. De plus, en étant coincée dans un système économique misant massivement sur le recours aux données (Couldry et Mejias, 2020; Sadowski, 2019; Zuboff, 2020), l'organisation n'aurait sans doute pas beaucoup d'intérêt à les considérer, puisque ce faisant elle irait à l'encontre de ses intérêts stratégiques concrets et immédiats pour des considérations immatérielles et hypothétiques sur lesquelles elle aura peu de moyens d'intervenir si ce n'est, comme je l'ai mentionné, en s'abstenant d'agir tout simplement. Il paraît peu probable que les organisations optent pour une telle avenue considérant les diverses injonctions qu'elles subissent à se transformer numériquement.

3.2.3 Les processus d'évaluation des risques et aspect constructiviste du risque à la vie privée

En plus des caractéristiques des risques et des préjudices portés à la vie privée qui minimisent leurs chances d'être considérés dans un processus d'évaluation, il paraît important de tenir compte également de leur dimension qualitative dans le processus d'évaluation. Si tous les éléments évoqués depuis le début de ce mémoire s'avèrent justes, les risques et les préjudices en matière de protection de la vie privée ne coïncideront jamais avec ceux encourus par l'organisation réalisant un projet. Ils correspondront plutôt à ceux que celle-ci fait courir à ses clients, à ses partenaires, aux citoyens ou, parfois, à la population au complet. Si l'évaluation visait à établir les risques de l'organisation, l'évaluateur pourrait la réaliser dans la perspective de l'expert détenant un savoir et traitant d'une problématique purement « technique ». Dans ce contexte, le professionnel réalisant une évaluation des risques et des préjudices à la vie privée pourrait se limiter à proposer des solutions « techniques » à son client — en l'occurrence, au promoteur du projet — et ce client pourrait suivre ou non les recommandations que l'évaluateur émet. Si l'évaluation visait la conformité légale (par exemple, l'avocat conseillant son client sur les mesures à mettre en place pour répondre aux exigences légales de protection des renseignements personnels) ou l'évaluation

de la sécurité des systèmes informatiques (par exemple, le professionnel en cybersécurité qui conseille le promoteur du projet sur les mesures technologiques et administratives à mettre en place pour réduire les risques de brèche de sécurité), cette posture professionnelle de l'évaluateur pourrait être envisagée. L'évaluateur pourrait, dans ce cas-ci, être l'« expert » décrit dans la typologie des postures professionnelles proposée par Georges Legault dans son livre *Professionnalisme et délibération éthique : manuel d'aide à la décision responsable* (2004, p. 31-32). Dans ce type de relation client-professionnel, comme le rappelle Legault, ce n'est pas la question de la meilleure décision que l'expert détermine, mais plutôt celle de la meilleure solution sur le plan technique : l'expert représente ici « celui qui dit la "vérité" sur un sujet ». Dans le contexte de la protection de la vie privée, il ne s'agit plus de savoir « est-ce que je dois aller de l'avant avec le projet, car la vie privée est protégée? » (une décision qui engage la responsabilité du promoteur du projet), mais plutôt « quels sont les mécanismes (juridiques, administratifs ou technologiques) que je dois mettre en place pour protéger la vie privée? » (des propositions techniques qui peuvent ou non être suivies par le promoteur).

Or, si l'on accepte l'analyse d'Helen Nissenbaum — celle qui fait de la vie privée une notion hautement contextuelle et intrinsèquement liée aux perceptions des personnes concernées — et si l'objectif du processus d'évaluation des risques et des préjudices est bien de protéger la vie privée de ces personnes, l'évaluation des risques devra tenir compte du point de vue de ces dernières étant donné qu'elles seules détiennent le dernier mot en ce qui concerne leur vie privée. Autrement dit, en partant de la prémisse que les risques ou les préjudices portés à la vie privée sont des constructions de la personne concernée, leur évaluation ne pourrait vraisemblablement reposer sur les épaules du spécialiste, ce dernier suggérant ensuite une série de correctifs ou de mesures techniques qui rendraient le projet acceptable du point de vue légal ou du point de la sécurité de l'information. L'avis des personnes directement visées par la problématique devrait être considéré dans l'évaluation des risques et des préjudices. Cela semblera d'autant plus important dans l'éventualité où les personnes concernées seront contraintes d'utiliser le système résultant du projet, par exemple s'il s'agit d'un projet gouvernemental dont l'usage sera imposé par voie légale ou

réglementaire.[45] Cela ne veut pas dire qu'une évaluation faite uniquement du point de vue de l'expert ne présenterait aucune utilité ou qu'elle raterait l'objectif de protéger la vie privée. Celle-ci contribuerait malgré tout à diminuer les chances qu'un risque se matérialise. Cela veut seulement dire qu'elle s'avérerait incomplète, parce que la prise en compte du point de vue de l'utilisateur ou du citoyen lui manquerait. La posture professionnelle qui semblerait dès lors la plus adéquate ou celle-là plus à même d'atteindre l'objectif de protéger la vie privée semble être celle de la coopération. C'est dire que, dans le contexte de cette évaluation, « le savoir pratique d'un professionnel est mis au service du "projet de vie" de la personne. » (Legault, 2004, p. 35) L'évaluateur, dans ce contexte, n'est pas l'expert qui dicterait ce qu'il est bon de faire ou non, mais plutôt l'expert qui accompagne le client dans le projet, en l'occurrence pour l'élaboration d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels. Toutefois, la question suivante est soulevée par cette réflexion sur la posture professionnelle de l'évaluateur : qui protège-t-il? Le promoteur du projet ou les personnes qui seront éventuellement concernées par celui-ci? Je reviens un peu plus loin sur cette question (section 3.3.2), car elle paraît primordiale dans le contexte d'une évaluation des risques et des préjudices à la vie privée.

Cette proposition n'a rien de bien novateur. Considérant les enjeux plus importants que pose l'intelligence artificielle, on retrouve déjà des recommandations faisant état de l'importance de la participation et de la collaboration dans la gouvernance des projets impliquant le recours à des algorithmes d'intelligence artificielle. Produite en 2018, la *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle* posait déjà la participation démocratique et l'inclusion, ainsi que la prise en compte de la diversité comme principes à respecter dans le déploiement de l'intelligence artificielle. Pour les auteurs de la Déclaration — elle-même conçue dans la délibération et par la participation citoyenne —, ces principes s'incarneraient notamment par la délibération portant sur les

[45] Du reste, l'impossibilité d'exercer son libre choix quant au recours à une réalisation constituerait en soi une atteinte sérieuse à la vie privée.

paramètres sociaux des systèmes à haut risque d'impacts sur la vie des citoyens et par la prise en considération de la pluralité et de la diversité sociale. *L'Organisation des Nations Unies pour l'éducation, la science et la culture* (UNESCO) pose que [l'italique est de moi] « [l]a participation des différentes parties prenantes tout au long du cycle de vie des systèmes d'IA [intelligence artificielle] est nécessaire pour garantir des approches inclusives de la gouvernance de l'IA, *permettant que les bénéfices soient partagés par tous*, et de contribuer au développement durable » (UNESCO, 2022). Elle promeut ainsi la gouvernance et la collaboration multipartites comme l'un des principes à respecter dans le cadre de l'utilisation de l'intelligence artificielle — tout comme le droit au respect de la vie privée et la protection des données par ailleurs — pour assurer le partage des bénéfices entre toutes les parties prenantes.

Pour un processus tel que l'ÉFVP, les considérations soulevées à la section précédente impliqueraient que l'évaluateur qui agirait en vase clos, sans passer par une consultation des personnes concernées par le projet, laisserait potentiellement de côté certains éléments importants de la dimension qualitative du risque et du préjudice porté à la vie privée. La décision de ne pas tenir compte du point de vue de ces dernières pourrait avoir un impact sur la détermination du champ d'application du processus d'évaluation et, en définitive, sur le calcul du rapport coût/bénéfice. Sur la base de quels critères l'arbitrage sera-t-il réalisé entre les bénéfices et les risques et préjudices portés à la vie privée? Le projet sera-t-il jugé acceptable du fait qu'il engendre au total plus de bénéfices que de risques pour l'ensemble de la société, sans tenir compte du fait qu'il peut engendrer des préjudices très importants pour un nombre restreint de personnes? Comme le rappelle Céline Kermisch :

> En effet, pour rendre compte de cette dernière [la dimension qualitative du risque], un élargissement du processus de gestion des risques s'impose : en parallèle à la quantification des risques, il convient d'introduire une étape supplémentaire, la « qualification des risques », c'est-à-dire une analyse destinée à mettre en lumière les enjeux qualitatifs en présence, qu'ils soient éthiques, politiques ou socioculturels. Cette étape pourrait être assurée par une démarche participative. (2012, p. 10)

Cependant, cette considération pour le caractère construit et culturel du risque et du préjudice à la vie privée soulève un commentaire. Il pourrait sembler exagéré d'exiger la participation citoyenne et la collaboration des parties prenantes pour tous les projets visés par l'obligation de réaliser une ÉFVP. En effet, le fait de rendre obligatoire la participation des citoyens ou des utilisateurs pourrait sembler exagérée si elle devait s'appliquer à l'ensemble des projets qui sont visés par l'obligation légale. Toutefois, je rappelle que l'envergure de l'ÉFVP devant être produite peut être modulée en fonction des critères de la sensibilité des renseignements personnels impliqués, de leur utilisation, de leur quantité, de leur répartition et de leur support. Je me permets de penser que la prise en compte du point de vue des citoyens ou des utilisateurs dans l'évaluation des risques et des préjudices portés à la vie privée demeure pertinente. Le fait de tenir compte de ces points de vue paraît particulièrement essentiel pour les projets de grande ou de très grande envergure (par exemple, pour un système de télésanté à l'échelle provinciale), pour les projets très structurants pour la société en général (par exemple, le projet d'identité numérique au Québec), pour ceux engendrant potentiellement des enjeux sérieux sur la vie privée des personnes (comme l'ont été les applications de suivi de contact utilisées au plus fort de la crise sanitaire) ou pour ceux impliquant des risques de discrimination pour des minorités (comme des algorithmes d'intelligence artificielle appliqués à la gestion des ressources humaines). On pourrait rétorquer et souligner que, pour connaître l'envergure d'un projet ou pour savoir s'il pose des risques sérieux sur la vie privée ou des risques de discrimination pour les minorités, encore faut-il l'évaluer, même partiellement. Autrement, comment entrevoir les problèmes qu'il peut poser? C'est peut-être là que l'obligation universelle de réaliser une ÉFVP peut trouver une certaine pertinence : dans sa forme la plus minimale, une ÉFVP devrait permettre de démontrer, en plus de la conformité aux lois, qu'il n'est pas jugé nécessaire de réaliser une évaluation des risques et des préjudices portés à la vie privée qui soit plus poussée. C'est-à-dire que l'organisation devrait être en mesure de justifier raisonnablement pourquoi ne juge-t-elle pas essentiel de pousser davantage le processus d'évaluation. Des critères permettant de juger ou non de cette nécessité pourraient s'inspirer de ceux proposés dans L'Énoncé de politique des trois conseils (EPTC) ou par le Groupe de travail « article 29 » dans ses lignes directrices pour la réalisation

des analyses d'impact relatives à la protection des données prévue au Règlement général sur la protection des données (RGPD). Pour l'EPTC, une « "recherche à risque minimal" s'entend d'une recherche où la probabilité et l'ampleur des préjudices éventuels découlant de la participation à la recherche ne sont pas plus grandes que celles des préjudices inhérents aux aspects de la vie quotidienne du participant qui sont associés à la recherche » (Gouvernement du Canada, 2018, p. 23). Le fait qu'une recherche soit considérée comme étant « à risque minimal » permet au comité d'éthique de faire l'économie d'une évaluation en plénière, celle-ci pouvant être réalisée par délégation par un ou deux membres du comité. Quant à eux, les neuf critères du RGPD ont été mentionnés antérieurement dans ce mémoire (voir page 39). Encore faut-il cependant être en mesure d'évaluer le projet à la lumière de ces critères. Or, même s'ils permettent d'envisager l'économie d'une évaluation plus exhaustive, la simple application de ces critères peut, pour certains projets, s'avérer complexe, par exemple si une technologie émergente est utilisée.

3.3 *QUELQUES ENJEUX ÉTHIQUES DE L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE*

3.3.1 L'aspect utilitariste des processus d'évaluation des risques et des préjudices

Au-delà des caractéristiques des risques et des préjudices portés à la vie privée qui les rapprochent des risques éthiques, l'activité d'évaluation des risques présente s'apparente elle-même à une activité éthique. L'évaluation des risques et des préjudices portés à la vie privée vise à établir un rationnel permettant de justifier qu'un projet a été entériné malgré les risques de préjudices qui seront causés effectivement ou qui pourraient être causés potentiellement à la vie privée des personnes concernées. Il s'agit en quelque sorte de préparer une plaidoirie en amont qui permettra au promoteur du projet de démontrer, advenant la matérialisation d'un risque engendrant un préjudice, que sa décision d'aller de l'avant fut prise de façon éclairée et responsable. Il s'agit de pouvoir dire aux personnes qui subissent le préjudice résultant de la matérialisation de ce risque que « nous y avions pensé, nous avions mis en place toutes les mesures pour que le risque ne se matérialise pas et nous

avons des mesures réparatrices à vous offrir pour pallier les conséquences ». Pour cette raison, les processus d'évaluation des risques et des préjudices en général s'appuient sur au moins trois principes proprement éthiques : le calcul utilitariste, le principe de précaution et la responsabilité des acteurs impliqués.

Le processus d'évaluation des risques et des préjudices relève d'abord d'un calcul utilitariste. Il vise, en définitive, à déterminer si une action que l'on s'apprête à poser est plus désirable et plus bénéfique que la somme des préjudices qu'elle engendre ou qu'elle pourrait engendrer advenant la matérialisation de certains événements (les risques). Il vise également à prévoir des mesures d'atténuation de ces préjudices et doit en tenir compte dans l'évaluation finale du calcul coût-bénéfice. Dans le cas des ÉFVP qui sont visées spécifiquement par ce mémoire, cette action évaluée consiste en la mise en œuvre d'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des renseignements personnels. Un tel projet sera considéré comme étant bon et acceptable si la somme des bénéfices escomptés s'avère supérieure aux risques et aux préjudices engendrés par sa réalisation, que les risques identifiés au projet demeurent potentiels ou qu'ils se matérialisent. Toutefois, dans une perspective proprement éthique, le calcul du rapport risques/bénéfices doit aussi tenir compte de la nature des bénéfices escomptés et de celle des conséquences probables, ainsi que des valeurs inscrites dans la conséquence et celles révélées par la décision d'aller de l'avant avec le projet malgré la présence de ces risques et de ces préjudices potentiels. Sans tomber dans les considérations et les subtilités méthodologiques que la mise en œuvre de la théorie utilitariste peut soulever (Salvat, 2020, p. 33-51), disons simplement que le projet sera considéré comme étant éthiquement bon et acceptable s'il maximise l'utilité générale.

Il semble donc juste de dire, comme le soulignent Raija Koivisto et David Douglas, que le fait de procéder à une évaluation de risques représente un geste essentiellement *éthique* en raison de l'action *évaluative* qui est accomplie : « Risk evaluation is the phase of the risk management process where the acceptance of the assessed risk is evaluated. Risk evaluation is a value and morality-based task. Usually, the (bigger) risk is acceptable if the resulting

outcome is valuable. » (Koivisto et Douglas, 2015, p. 4) Aussi, disent-ils, « [r]isk assessment is motivated by the desire to reduce the possibility of harm occurring. » (Koivisto et Douglas, 2015, p. 6) Je rappelle, pour compléter cette citation que l'évaluation des risques et des préjudices ne vise pas uniquement à réduire ou à éliminer la *possibilité* qu'un préjudice se matérialise, mais cherche en parallèle à mettre en place des mesures visant à *atténuer les impacts* que ce préjudice pourrait avoir. L'intention demeure la même : réduire à la fois les probabilités et les impacts des préjudices engendrés potentiellement par une activité, un projet, un programme ou une action, dans l'espoir d'en maximiser les bénéfices. Un gain suffisamment grand militera en faveur de la réalisation de ce projet ainsi jugé acceptable. Dans les mots de Koivisto et Douglas, le processus d'évaluation du risque « captures the intuition (expressed in adages like 'it is better to be safe than sorry') that it is better to avoid significant harms than to address them after they have occurred. » (Koivisto et Douglas, 2015, p. 7) Ainsi, le fait de procéder à une évaluation des risques s'appuie sur l'idée qu'il vaut mieux prévenir que guérir, et qu'un projet ne peut être éthiquement justifié si sa réalisation ne tient pas compte des risques engendrés pour des tiers.

Le second principe éthique qui est mobilisé par les processus d'évaluation des risques — ou qui devrait l'être dans le meilleur scénario — est le principe de précaution. La COMEST propose la définition suivante du principe de précaution appliqué aux innovations technologiques et scientifiques : « Lorsque des activités humaines risquent d'aboutir à un danger moralement inacceptable, qui est scientifiquement plausible, mais incertain, des mesures doivent être prises pour éviter ou diminuer ce danger. » (COMEST, 2005, p. 14) L'existence d'un processus d'évaluation est justifiée par cet impératif moral de minimiser les risques qu'un événement se matérialise et qu'il engendre des effets néfastes indésirables sur les personnes concernées. Pour le cas qui nous occupe, le Québec a jugé suffisamment importants les risques et enjeux soulevés globalement par l'utilisation des renseignements personnels pour ériger en obligation des mécanismes visant à en atténuer les impacts, mettant ainsi en œuvre le principe de précaution. Finalement, tout le processus d'évaluation sert à la prise de décision quant à l'acceptabilité d'un projet. Ainsi, il implique à la fois la responsabilité professionnelle de l'évaluateur envers son client et celle du décideur

envers l'utilisateur éventuel du projet. C'est ainsi que le processus d'évaluation de risques et de préjudices engage la responsabilité des différents acteurs impliqués dans sa réalisation. L'implication de ces trois principes éthiques soulève des enjeux particuliers dans le contexte des évaluations des risques et des préjudices portés à la vie privée.

L'aspect utilitariste du processus soulève d'abord la question de l'identité des bénéficiaires et des personnes concernées par les préjudices potentiels. Comme le souligne Koivisto et Douglas, la démarche évaluative est enclenchée en amont du processus d'évaluation des risques à proprement parler. Une première sélection des risques est effectuée à l'étape de fixer les paramètres de l'exercice, lorsque le « terrain de jeu » du processus d'évaluation des risques est déterminé, au moment où le domaine d'application est établi. Le choix du domaine d'application est lié, je le rappelle, aux objectifs qui sont visés par le processus d'évaluation et qui peuvent être stratégiques, financiers, juridiques, etc. Il a été mentionné à plusieurs reprises déjà que les risques à l'étude varieront considérablement en fonction des objectifs. Dès ce premier tri, les risques et les préjudices portés à la vie privée dont la nature s'apparente davantage aux risques éthiques (comme des risques engendrant des impacts psychologiques, des discriminations ou des entraves à l'autonomie des personnes) pourront être écartés si l'évaluation poursuit des objectifs qui s'en détournent.

La démarche évaluative se poursuit au moment d'établir le niveau minimal d'impact ou de probabilité des risques suffisamment importants pour être considérés. Ce seuil fait référence à la notion de « limite de la préoccupation » (« limit of concern ») mentionnée par Koivisto et Douglas : « Risks that are regarded as being too insignificant are called de *minimis risks*. This can be regarded as a 'limit of concern' or a threshold that determines whether potential risks should influence our judgment. » (Koivisto et Douglas, 2015, p. 9) Seuls les risques et les préjudices qui surpassent ce seuil seront considérés dans le processus évaluatif, alors que les autres seront volontairement écartés ou simplement non identifiés. Il s'agit là d'un autre geste évaluatif fondamental. L'étape suivante consiste à discriminer, dans le lot des risques qui surpassent la limite de préoccupation, ceux qui sont acceptables de ceux qui ne le sont pas.

L'activité de déterminer tous ces seuils repose en partie sur les présupposés et les biais de l'évaluateur : « This limit is arbitrary and may differ between various risk assessors and regulators. It is important to recognize that the level of acceptable risk is not based solely on scientific evidence and will necessarily reflect political, social, and ethical beliefs about risk. » (Koivisto et Douglas, 2015, p. 9) Pour reprendre les termes de Céline Kermisch, l'ensemble du processus d'évaluation est influencé par un filtre socioculturel et subjectif propre à l'évaluateur :

> Dans le paradigme nature-culture[46], un même danger peut donner lieu à plusieurs interprétations, parmi lesquelles des risques de degré variable. Par exemple, le filtre socioculturel opère de manière très différente vis-à-vis des risques associés à l'énergie nucléaire, selon qu'ils sont estimés par le fournisseur d'énergie ou par des militants antinucléaires. (2012, p. 5)

Comme le mentionne la COMEST, d'autres variables que la probabilité et l'impact peuvent également entrer en ligne de compte dans l'évaluation :

> La mesure dans laquelle on considère qu'un risque est acceptable ou non dépend non seulement de l'ampleur du dommage et de la probabilité que ce dommage se produise, mais encore d'autres dimensions du risque. Un risque donné tend à être considéré comme moins acceptable si la contrôlabilité (perçue) de ses conséquences est plus faible, si la nature des conséquences est mal connue et épouvantable, si l'on est exposé au risque sans le vouloir, si les avantages de l'activité envisagée sont moins nets et plus faibles, si les effets sont plus aigus et plus proches dans l'espace et dans le temps, si le risque et les avantages sont inéquitablement répartis et si le danger probable est intentionnel. (2005, p. 28)

Autrement dit, la discrimination entre les risques non considérés, les risques acceptables et les risques inacceptables passe inévitablement au crible des valeurs, des préférences et des préjugés de l'évaluateur.

Il y aurait donc des moments évaluatifs fondamentaux dans la réalisation d'un exercice de risque : un premier qui a lieu lorsqu'est déterminée la nature des événements qui seront

[46] Le terme « nature » faisant ici référence à l'événement qui survient dans l'absolu, indépendamment de la perception qu'une personne peut en avoir.

considérés dans l'évaluation (laissant voir que certaines dimensions touchées par un projet ne sont pas sujet de préoccupation pour l'évaluateur) et un second qui a lieu lorsque les paramètres d'évaluation des risques sont déterminés (paramètres qui sont influencés, de l'avis de Koivisto, Douglas et de la COMEST, par l'évaluateur lui-même).

Tout ce discours sur le caractère utilitariste du processus d'évaluation des risques nous mène à l'étape suivante du processus : la prise de décision en elle-même. Koivisto et Douglas soulignent qu'il y a une différence éthique importante entre le fait de prendre une décision qui fait courir un risque pour soi-même et une décision qui expose un tiers à un risque. En citant Sven Ove Hansson (Hansson, 2004; Koivisto et Douglas, 2015), ils rappellent certaines dimensions éthiquement pertinentes de la prise de décision qui engendre des risques :

- L'exposition au risque est-elle intentionnelle (le décideur ou les personnes concernées sont informés et conscients du risque) ou non intentionnelle (le risque n'est pas connu du décideur ou des personnes concernées, par manque de connaissances ou par une mauvaise lecture de la situation)?

- L'exposition au risque est-elle volontaire (toutes les personnes concernées peuvent accepter ou non de courir le risque) ou imposée (les personnes concernées ne peuvent s'extraire du processus menant à l'exposition au risque, par exemple dans le cadre d'un projet gouvernemental applicable à l'ensemble de la population)?

Pour les situations où la décision d'accepter le risque est imposée par un tiers (par le gouvernement par exemple), une personne concernée peut quand même adhérer à cette prise de risques (elle en comprend les tenants et aboutissants et les accepte), ou elle peut les subir, mais ne pas adhérer aux principes et justifications qui ont mené à l'explication du risque. Les différentes réponses qui seront données à ces questions dans le cadre d'un projet spécifique vont venir influencer le niveau de responsabilité du décideur dans l'acceptation du risque.

Ainsi, la responsabilité du promoteur d'un projet ne sera pas engagée de la même façon s'il offre un service auquel une personne peut souscrire volontairement, en acceptant

pour elle-même de courir les risques qui y sont associés ou s'il fait la promotion d'un projet dont l'utilisation sera imposée. Pensons par exemple à un projet impliquant des modifications législatives qui mènerait aux partages de données gouvernementales sans le consentement des personnes concernées. Plus le niveau de responsabilité augmente, plus les processus menant à la prise de décision — dont font partie les processus d'évaluation des risques — gagnent à être inclusifs et transparents, parce qu'ils diminuent les chances que des risques soient encourus non intentionnellement (par une meilleure identification et une meilleure connaissance des enjeux potentiels) et parce qu'ils favorisent l'adhésion et les chances que l'exposition aux risques soit acceptée même si elle est, dans les faits, imposée. Au contraire, dans un contexte où l'exposition aux risques serait imposée et les risques moins connus (parce que mal identifiés ou mal communiqués aux personnes), la responsabilité des acteurs décisionnels sera engagée davantage s'ils ont accepté d'exposer intentionnellement des tiers à des risques, malgré l'existence d'une incertitude résiduelle potentiellement importante et en dépit du fait que ces tiers pourraient ne pas adhérer au projet.

La recherche du consentement paraît incompatible avec les projets menant à une exposition imposée à des risques. D'un point de vue pratique, il est illusoire de penser obtenir le consentement individuel de toutes les personnes concernées par un projet lorsque celui-ci est imposé à toute une population ou sous-population. C'est d'autant plus vrai à l'ère de l'intelligence artificielle, alors que les algorithmes peuvent désormais généraliser leurs effets à des populations non visées par le projet et dont les impacts peuvent s'étendre à l'ensemble de la population. Or, le consentement est la pierre angulaire de plusieurs mécanismes de protection de la vie privée, notamment en matière de protection des renseignements personnels et de l'éthique de la recherche. Comment dès lors concilier cet idéal de l'autonomie individuelle cher à nos sociétés libérales occidentales avec les impératifs qui peuvent gouverner la prise de décision? Pour pallier cette impossibilité de l'obtention du consentement, la recherche de l'adhésion et du compromis par le dialogue, l'échange, la collaboration et la transparence avec ces personnes paraît plus respectueuse de leur autonomie. Si le projet touche un nombre de personnes trop important, voire des populations

entières, le dialogue des représentants de ces personnes est susceptible d'amoindrir les effets délétères de la mise en œuvre du projet.

Pour résumer, le processus d'évaluation des risques est un acte éthique, car il implique de porter dans l'immédiat un jugement sur la valeur d'un projet à la lumière des possibles qu'il engendre. En outre, l'évaluation des risques s'effectue à l'intérieur d'une sorte *de crible évaluatif*, un processus où les risques passent différents critères : celui du champ d'application, celui de la limite de préoccupation, puis celui du seuil de tolérance. Cette évaluation se réalise à partir d'une grille d'analyse qui n'est pas sans être influencée par les valeurs et les intérêts propres à l'évaluateur. L'action d'évaluer le risque présente deux phases évaluatives distinctes. Une première phase s'effectue au moment d'établir les paramètres de l'évaluation, et une deuxième au moment d'évaluer les risques en eux-mêmes. Suivant l'élagage des risques, puis leur évaluation, les différentes prises de décision qui découleront de l'exercice d'évaluation engageront la responsabilité du décideur qui prend sur lui d'entériner le projet malgré la subsistance de risques. Le processus d'évaluation des risques vise à alimenter la réflexion entourant la décision d'aller ou non de l'avant avec le projet générateur de risques. L'organisation prend ensuite la décision en acceptant de tolérer que des risques subsistent pour elle-même (elle prend le risque [« taking risk »]) ou en acceptant d'exposer un tiers à ces risques (« risk exposure »). Le niveau de responsabilité variera selon que l'exposition au risque est a) connue ou non par l'évaluateur et le décideur, et b) connue ou non par la personne concernée. Elle variera également selon que cette exposition est c) volontairement choisie ou non par l'évaluateur (advenant que le risque en question n'a pas été identifié), et d) assumée ou subite par la personne concernée, que celle-ci soit e) au courant du risque ou en est inconsciente. Ce dernier peut partager cette responsabilité avec la personne concernée par le projet en l'informant au mieux des risques subsistants, de manière à forger un consentement (implicite ou non) qui serait le plus éclairé possible. Ultimement, les utilisateurs du système d'information évalué seront également appelés à faire leur propre « gestion de risques » en déterminant, à partir de leur propre crible évaluatif, si le recours à l'outil résultant du projet leur apporte plus de bénéfices que les risques engendrés par celui-ci.

Cette dernière gestion de risques effectuée par le citoyen ou l'utilisateur final du projet peut faire l'objet de deux considérations. Elle requiert d'abord que les personnes soient suffisamment éclairées sur les tenants et aboutissants du projet pour en faire une évaluation adéquate. Cela exige d'une part que l'organisation qui met en œuvre le projet soit suffisamment transparente pour fournir l'information requise et nécessaire à l'évaluation, puis que la personne qui la fera ait elle-même le temps et les compétences nécessaires pour faire celle-ci de manière satisfaisante. Ce dernier point introduit l'idée — que j'aborde plus spécifiquement dans la prochaine section — que l'évaluateur des risques et des préjudices portés à la vie privée se trouve davantage dans une relation professionnelle avec l'utilisateur final du projet (le citoyen ou le consommateur) plutôt qu'avec l'organisation pour qui il réalise l'évaluation. La seconde considération concerne les caractéristiques des risques et des préjudices portés à la vie privée soulevées dans les sections 3.2.1 et 3.2.2, à savoir que ceux-ci sont souvent négligeables, non ressentis et collectifs plutôt qu'individuels. Si l'évaluateur qui œuvre pour une organisation est influencé de multiples façons par des préjugés et des inclinaisons personnelles, l'utilisateur final l'est tout autant. Or, comme le souligne Solove:

> With many privacy decisions, the benefits are immediate and concrete. People can receive access to entertainment, news, and information. They can obtain great services and products. They can use convenient and useful technologies. On the privacy side is a risk that is often vague, abstract, and speculative. (2022, p. 11)

Ainsi, face à la commodité offerte par les technologies, les considérations de protection de la vie privée peuvent facilement passer au second plan. Les différents mythes entourant la vie privée (section 2.4.1), notamment le « nothing to hide argument », alimentent également cet écart important entre la perception du préjudice potentiel et les bénéfices immédiats et tangibles offerts par une solution technologique. En effet, pourquoi une personne se préoccuperait-elle de risques hypothétiques et potentiellement négligeables, surtout si elle considère ne pas avoir de secrets inavouables? Ainsi, les risques et les préjudices portés à la vie privée sont, en raison de leur nature, susceptible d'avoir peu d'impact dans un processus décisionnel.

3.3.2 La posture professionnelle des évaluateurs des risques et des préjudices en matière de protection de la vie privée

Toutes ces considérations sur la nature éthique de l'évaluation des risques et des préjudices me mènent à poser la question de l'expertise et des compétences de la personne qui réalise cette évaluation, ainsi que celle de la posture professionnelle à privilégier. En effet, la complexité inhérente de la notion de protection de la vie privée et les connaissances juridiques, technologiques et éthiques requises laissent croire que ce processus d'évaluation ne pourrait pas être confié à n'importe qui. De plus, en considérant l'influence du contexte à la fois sur le jugement de l'évaluateur et sur la perception de ce qui constitue un risque ou un préjudice porté à la vie privée, la posture professionnelle de l'expert en matière de protection de la vie privée devrait relever davantage de la coopération avec les personnes concernées par le projet et moins celle du paternalisme ou du rôle d'expert de contenu (Legault, 2004).

Il paraît d'abord important de rappeler la distinction qui peut exister entre l'évaluateur et la personne qui prend actuellement la décision d'aller de l'avant ou non avec un projet malgré l'existence de risques. Ces derniers peuvent parfois s'avérer être la même personne. Cette situation arrivera certainement assez fréquemment pour les plus petites entreprises aux ressources limitées. Néanmoins, la COMEST souligne qu'il est préférable qu'il y ait séparation fonctionnelle entre les deux rôles (COMEST, 2005, p. 28). Juridiquement, la responsabilité d'accepter ou non les résultats de l'ÉFVP reposera vraisemblablement sur les épaules d'une seule et même personne, soit la dirigeante ou le dirigeant de l'organisation. Il semblerait tout aussi logique que la personne désignée comme responsable de la protection des renseignements personnels dans une organisation l'assisterait dans cette prise de décision. Pour les organismes publics, la Loi sur l'accès prévoit que la personne détenant la plus haute autorité administrative au sein d'une organisation publique porte ce titre de responsable des renseignements personnels, mais celle-ci peut déléguer cette responsabilité à un membre de son personnel. Dès septembre 2022, la Loi sur le privé prévoira que toute personne qui exploite une entreprise sera elle aussi désignée comme personne responsable de la protection des renseignements personnels qu'elle détient, ou qu'elle pourra déléguer

cette responsabilité à un membre de son personnel. Si cette personne n'a pas les compétences nécessaires pour réaliser seule l'exercice d'évaluation des risques et des préjudices — ce qui paraît probable pour les projets d'envergure ou impliquant l'utilisation de renseignements personnels sensibles ou des technologies avancées — il s'avérera important qu'elle puisse s'appuyer sur une évaluation produite par des personnes jugées dignes de confiance.

La possibilité que l'évaluateur et le décideur soient la même personne ou celle que l'évaluateur soit un salarié ou un contractuel qui doit défendre les intérêts de son employeur soulèvent des questions quant aux conflits d'intérêts et à la partialité d'un processus d'évaluation des risques. De tels risques peuvent s'insinuer à toutes les étapes évaluatives du processus de gestion des risques et des préjudices : de la détermination du champ d'application — ce qui peut mener à l'exclusion de plusieurs risques pourtant réels — à la détermination des niveaux de risques acceptables ou à la décision de prendre en compte ou non la dimension qualitative des risques et des préjudices portés à la vie privée. C'est toute la question de l'impartialité de l'évaluateur qui se pose ici et celle de l'objectivité de l'évaluation des risques qu'il effectuera. La question pourrait se formuler ainsi : l'intérêt du public sera-t-il considéré à juste titre par l'évaluateur ou bien seul l'intérêt de son client prévaudra? La pertinence ou l'intégrité d'une évaluation réalisée uniquement au bénéfice de l'organisation serait contestable, en raison notamment de l'influence des filtres socioculturels et du tri évaluatif sur tout le processus d'évaluation du rapport coûts/bénéfices. *A contrario*, une évaluation appuyée uniquement sur les intérêts des personnes concernées pourrait peut-être nuire davantage plutôt que d'aider à tirer le plus de bénéfices de l'utilisation des nouvelles technologies. Nous pouvons penser qu'une réponse mitoyenne serait préférable : l'évaluateur devrait jouer le rôle de médiateur éclairé et impartial qui tient compte à la fois des intérêts du promoteur du projet et de ceux des personnes concernées. Il est possible de penser que la professionnalisation du travail d'évaluateur en matière de protection de la vie privée permettrait de garantir jusqu'à un certain point cette prise en compte d'intérêts coexistants, et parfois divergents.

Comme ce sont les objectifs de l'organisation qui viennent déterminer le champ d'application du processus d'évaluation, celui-ci pourrait indûment être influencé par les intérêts de l'organisation, surtout en l'absence de contraintes ou d'attentes externes venant préciser ce qui est attendu de l'exercice de gestion des risques, ce qui est actuellement le cas en ce qui concerne l'obligation de réaliser des ÉFVP pour les projets technologiques. Cette obligation, pour l'instant, s'appuie sur l'hypothèse que les organismes publics et les entreprises privés sauront s'autoréguler et sauront juger adéquatement des risques qu'ils font courir aux personnes concernées. Il faudra voir dans quelle mesure cette autorégulation s'avère possible dans les faits.

J'ai déjà soulevé l'idée que le profil de compétences de la personne idéale pour réaliser cette évaluation fera appel à de nombreuses qualifications qu'il paraît peu probable de retrouver dans une même personne. En effet, cette personne idéale devrait pouvoir établir que le projet évalué est a) conforme aux lois applicables, b) que les mesures de sécurité technologiques et administratives mises en œuvre pour protéger les renseignements personnels seront suffisantes et proportionnelles par rapport à leur sensibilité et advenant que ces derniers doivent également être évalués c) que les enjeux éthiques auront été adéquatement considérés dans l'évaluation, ce qui implique d'avoir consulté toutes les parties prenantes au projet ou, du moins, leurs représentants. J'ajouterais un autre élément à ces considérations : si une évaluation des risques et des préjudices portés à la vie privée qui se veut véritablement protectrice de la vie privée doit passer par une évaluation plus large des risques éthiques engendrés par un projet (voir section 2.4.1), encore faut-il que l'évaluateur soit sensible à la dimension éthique des problématiques qu'il évalue, faute de quoi l'évaluation risquera de n'être que juridique, technique, financière, etc. Pour reprendre les termes d'André Lacroix, d'Allison Marchildon et de Luc Bégin (2017), l'évaluateur doit pouvoir éprouver un certain « déséquilibre éthique » et il doit être en mesure d'entrer en « situation éthique » lui permettant de percevoir les enjeux proprement éthiques du projet sur lequel il réfléchit, faute de quoi ces derniers passeront vraisemblablement inaperçus. Pour ces raisons, du seul point de vue de la faisabilité, il paraît plus réaliste de penser que l'ÉFVP

sera réalisée avec la collaboration de plusieurs personnes au sein d'une même organisation ou en ayant recours à des ressources externes spécialisées dans ce genre d'exercice.

Avant d'aller plus loin dans l'exploration de la posture professionnelle qu'un évaluateur des risques et des préjudices en matière de protection de la vie privée devrait adopter, il est également possible de questionner l'existence même d'une telle profession. Est-ce que les tâches effectuées par un évaluateur des risques et des préjudices portés à la vie privée pourraient qualifier cette fonction à titre de profession au sens du *Code des professions* (RLRQ, chapitre C-26)? Je rappelle d'abord les conditions de professionnalisation prévues par la loi québécoise [l'italique est de moi] :

> 1° les *connaissances requises* pour exercer les activités des personnes qui seraient régies par l'ordre dont la constitution est proposée;
>
> 2° le *degré d'autonomie* dont jouissent les personnes qui seraient membres de l'ordre dans l'exercice des activités dont il s'agit, et la difficulté de porter un jugement sur ces activités pour des gens ne possédant pas une formation et une qualification de même nature;
>
> 3° le *caractère personnel des rapports entre ces personnes et les gens recourant à leurs services*, en raison de la confiance particulière que ces derniers sont appelés à leur témoigner, par le fait notamment qu'elles leur dispensent des soins ou qu'elles administrent leurs biens;
>
> 4° la *gravité du préjudice* qui pourrait être subi par les gens recourant aux services de ces personnes par suite du fait que leur compétence ou leur intégrité ne seraient pas contrôlées par l'ordre;
>
> 5° le *caractère confidentiel des renseignements* que ces personnes sont appelées à connaître dans l'exercice de leur profession.

En considérant tout ce qui a été mentionné depuis le début de ce mémoire, il paraît indubitable que le niveau et la variété des connaissances requises pour tenir les exercices d'évaluation des risques et des préjudices sont suffisants pour envisager que cette activité convient à la notion de « profession ». L'applicabilité des quatre autres critères pourrait faire l'objet de discussions plus étendues. De prime abord, nous pouvons penser que l'évaluateur devrait

pouvoir jouir d'une autonomie suffisante pour que son évaluation atteigne un niveau d'objectivité suffisant aux yeux d'un observateur externe. Aussi, le fait qu'une mauvaise évaluation des risques pourrait engendrer des préjudices autant pour l'organisation (des préjudices financiers, juridiques ou stratégiques) que pour les consommateurs ou les citoyens (des préjudices portés à leur vie privée) souligne l'importance de la confiance qu'un client de l'évaluateur doit pouvoir accorder à ce dernier. L'applicabilité de l'avant-dernier critère peut paraître sujette à débat, mais il demeure pertinent dans le contexte à mon avis. Même si la gravité des préjudices portés à la vie privée est souvent négligeable (comme je l'ai soulevé à la section précédente), l'organisation qui expose des personnes à ces risques demeure quand même sujette à d'importants préjudices advenant la matérialisation d'un risque porté à la vie privée de ses clients ou des citoyens, notamment des préjudices financiers, juridiques et réputationnels. Finalement, pour faire une gestion adéquate des risques, l'évaluateur doit avoir accès à de l'information sensible et stratégique pour l'organisation, notamment de l'information portant sur les mécanismes de sécurité de l'information et de cybersécurité. La divulgation de telles informations pourrait, dans certains cas, s'avérer catastrophique pour l'organisation et, plus largement, pour la société en général. Pensons notamment au contenu d'une évaluation qui serait faite pour un projet de nature militaire ou visant la sécurité publique.

S'il est fait mention dans ce mémoire des conditions de professionnalisation prévues au *Code des professions*, ce n'est pas pour proposer qu'un ordre professionnel devrait être créé pour les évaluateurs des risques et des préjudices en matière de protection de la vie privée. Une analyse visant à établir l'opportunité ou non de professionnaliser cette fonction resterait à faire entièrement. Il est intéressant toutefois de mentionner qu'il existe déjà des associations ou regroupements qui ont pour objet le développement des compétences en matière de protection de la vie privée. Au Québec, l'Association des professionnels en accès à l'information et en protection de la vie privée (AAPI) joue un tel rôle pour les organismes publics. L'*International Association of Privacy Professionals* (IAPP) occupe une fonction similaire à l'international.

Le fait de référer au Code des professions sert plutôt d'amorce pour une réflexion sur les valeurs qui devraient potentiellement guider les personnes exerçant les fonctions d'évaluateur des risques et des préjudices en matière de protection de la vie privée. Il faut, comme le rappelle Legault, se poser la question de l'idéal qui devrait animer une profession :

> Définir le professionnalisme, c'est entrer dans l'univers de « ce qui devrait être » et non de ce qui est. En effet, lorsqu'on cherche à préciser nos attentes à l'égard d'un professionnel, on ne décrit pas ce qu'il fait, mais ce qu'il devrait être parce qu'il est un professionnel. Précisez le professionnalisme, c'est identifier les différentes qualités qui devraient animer l'exercice de la profession. (2004, p. 41)

En l'occurrence, il s'agit de se poser la question de ces qualités dont l'évaluateur des risques et des préjudices portés à la vie privée devrait pouvoir se réclamer.

C'est la nature de la relation professionnelle qu'il faut définir ici, ce qui ramène toute la question de l'identité du client de l'évaluateur des risques et des préjudices portés à la vie privée. Considérant tous les éléments qui ont été soulevés depuis le début de ce mémoire, il est possible de penser que, comme pour les professions inscrites dans un ordre professionnel, la sécurité du public pourrait être au cœur de cet idéal. D'autres valeurs pourraient également être mobilisées dans la réalisation des tâches de ces évaluateurs. Pensons notamment à l'objectivité et à l'intégrité des processus d'évaluation qui reposent au moins en partie sur le maintien d'une saine distance entre le processus d'évaluation et la prise de décision. Pensons également à la confidentialité qui est une condition essentielle au maintien du lien de confiance entre l'évaluateur et le promoteur du projet. Les valeurs mises de l'avant par l'Énoncé de politique des trois conseils pourraient être également considérées, soit le respect des personnes, la préoccupation pour le bien-être et la justice (Gouvernement du Canada, 2018, p. 6-9).

Comme le mentionne Legault, « [s]ans ces valeurs et sans mécanismes pour assurer le professionnalisme de ses membres, une profession peut rapidement perdre toute crédibilité » (Legault, 2004, p. 49). Différents mécanismes pourraient être envisagés pour favoriser la transmission et l'intégration de ce contenu axiologique. Avant d'en venir à proposer la création d'un ordre professionnel, d'autres avenues pourraient être envisagées, comme la

mise en place d'un processus de certification ou la création de programmes de formation dédiés à la protection de la vie privée dans un contexte technologique. Ces différents mécanismes pourraient participer à la mitigation des risques liés à l'exercice de la fonction d'évaluateur des risques et des préjudices en matière de protection de la vie privée en rappelant clairement quelles sont les valeurs qui devraient guider le professionnel dans ses actions.

3.3.3 Remettre en question la faisabilité de l'obligation de produire des évaluations des facteurs relatifs à la vie privée

L'intégration de la dimension proprement éthique dans l'évaluation des facteurs relatifs à la vie privée (ÉFVP) nécessitera du temps afin de tenir les réflexions et les discussions nécessaires à la réalisation d'un exercice de qualité, répondant véritablement à l'objectif. Elle nécessitera également d'avoir une certaine ouverture à la dimension éthique des préjudices causés par les risques à la vie privée. En outre, l'organisation devra pouvoir compter sur un évaluateur qui détiendra des connaissances et des compétences juridiques, technologiques et éthiques spécialisées lui permettant d'évaluer adéquatement un projet informatique du point de vue de la protection des renseignements personnels et de la sécurité de l'information. Même sans ouvrir le champ d'application à la dimension éthique, il faudra tout de même pouvoir établir la conformité légale du projet, ce qui implique une évaluation des mesures en matière de sécurité de l'information. Or, une telle évaluation nécessitera minimalement d'avoir un niveau acceptable de connaissances dans le droit applicable à la protection de la vie privée, en sécurité de l'information et en cybersécurité. Dans le contexte actuel, il est possible de douter de la disponibilité d'évaluateurs en nombre suffisant pour répondre à la demande éventuelle.

Il paraît très difficile d'estimer adéquatement le nombre d'ÉFVP qui aura à être réalisée dans les prochaines années. Il n'y a pas de précédent juridique tout à fait comparable sur lequel baser une estimation. *La Directive sur l'évaluation des facteurs relatifs à la vie privée* du gouvernement fédéral ne s'applique qu'aux institutions fédérales et ne touche pas les entreprises du secteur privé. Tout de même, alors qu'Immigration, Réfugiés et

Citoyenneté Canada recense 5 ÉFVP pour la seule année 2019-2020, l'Agence du revenu du Canada indique en avoir réalisé 14 pour 2021-2022 (ARC, 2022; IFCC, 2020). Quant à elle, bien qu'elle s'applique aux entreprises de tous acabits, l'obligation européenne de réaliser une analyse d'impact à la protection des données (AIPD) est limitée aux traitements susceptibles « d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». Comme je l'ai mentionné à la section 1.3, l'obligation de produire une AIPD est conditionnelle à l'application de neuf critères visant à établir un niveau minimal de risque aux droits et libertés et, en plus, les autorités de contrôle de chaque pays membre de l'Union européenne peuvent établir une liste d'exceptions qui vient atténuer le nombre d'analyses devant être produites. En plus de ces critères qui permettent de réduire le nombre réel d'AIPD à réaliser, l'Union européenne n'oblige pas la diffusion de ces évaluations par les organisations et il n'y a pas de registre qui permettrait de savoir dans quelle proportion des AIPD sont réalisées. Ainsi, à l'égard de la nouvelle obligation québécoise, il est seulement possible de supputer des estimations à partir des données indirectes, comme le nombre d'organisations assujetties à cette nouvelle obligation.

Rappelons d'abord que l'obligation de produire des ÉFVP touchera un très grand nombre d'organisations ce qui soulève des considérations sur sa faisabilité concrètement. Les entreprises privées représentent à elles seules un nombre non négligeable d'organisations susceptibles d'avoir à réaliser un projet assujetti à l'obligation de produire une ÉFVP. Comme le stipule la CAI :

> Le terme « entreprise » réfère à l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services (art. 1525 du Code civil du Québec [CCQ-1991]). Cette définition s'étend notamment à l'entreprise individuelle (travailleur autonome), à la société par actions (compagnie), à la société en nom collectif (S.E.N.C.), à la société en commandite (S.E.C.), à la société en participation, à la personne morale sans but lucratif, au syndicat de copropriété, à l'association (p. ex. : syndicat), au groupement de personnes (p. ex. : consortium) ou à une fiducie exploitant une entreprise à caractère commercial. (2021, note 9)

Selon des données de l'Institut de la statistique du Québec (ISQ), il y aurait près de 880 000 entreprises avec ou sans employés au Québec (879 767 selon les données de décembre 2020). De ce nombre, 611 420 entreprises ne comptent aucun salarié — il s'agit d'entreprises individuelles — et 267 600 autres sont considérées comme étant des PME (petites ou moyennes entreprises) dont 262 534 sont en fait de petites entreprises qui comptent moins de 100 employés[47]. (ISQ, 2021a) Il est possible de douter que ces entreprises aient les équipes nécessaires pour réaliser adéquatement toutes les composantes d'une ÉFVP. Par ailleurs, la taille de l'organisation ne paraît pas être un très bon prédicteur quant à l'envergure des projets informatiques qu'elle pourrait avoir à réaliser. Nombre d'entreprises en démarrage peuvent faire usage de très grandes quantités de renseignements personnels ou faire usage de renseignements très sensibles sans toutefois pouvoir compter sur un grand nombre d'employés ou sur des ressources juridiques, technologiques ou éthiques appropriées. Clearview AI, cette compagnie dont l'affaire impliquant la collecte et l'utilisation illicite de millions de photos au Canada a été soulevée en page 87, fut au départ l'idée d'un seul homme. Or, en application du principe de protection de la vie privée dès la conception, l'ÉFVP portant sur son système de reconnaissance faciale aurait dû être produite en amont du développement de la solution et non en aval, au moment de sa commercialisation. Au niveau des organisations publiques, rappelons que la Loi sur l'accès s'applique à un très grand nombre d'organismes également. Y sont assujettis les organismes gouvernementaux (article 4), les organismes municipaux (article 5), les organismes scolaires[48] (article 6) et les établissements de santé ou de services sociaux[49] (article 7). La consultation du répertoire disponible sur le site Internet de la CAI[50], un document de

[47] Au Canada, une entreprise est qualifiée de petite ou de moyenne entreprise si elle compte moins de 500 employés. La petite entreprise en compte moins de 100. (Gouvernement du Canada, 2022)

[48] Incluant les cégeps, les universités et les établissements d'enseignement privés subventionnés.

[49] Incluant les centres locaux de services communautaires, les centres hospitaliers, les centres de protection de l'enfance et de la jeunesse, les centres d'hébergement et de soins de longue durée (CHSLD) et les centres de réadaptation.

[50] Accessible à l'adresse suivante : https://www.cai.gouv.qc.ca/liste-des-organismes-assujettis-et-des-responsables-de-lapplication-de-la-loi-sur-lacces/.

260 pages, permet d'obtenir un aperçu de la variété des quelque 3000 organisations publiques assujetties à l'obligation de produire des ÉFVP.

En partant de l'hypothèse que, sur une base annuelle, seulement 1 % des entreprises privées et des organismes publics québécois auront à produire une ÉFVP pour un projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels — hypothèse très conservatrice si l'on considère les innombrables discours réaffirmant l'importance de miser sur la transformation numérique des organisations — et en excluant de l'équation les autres occurrences où une ÉFVP est requise[51], il y aurait plus de 8000 de ces évaluations qui devraient être produites chaque année. N'oublions pas que, malgré la possibilité prévue dans les lois de moduler l'évaluation en fonction de « la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support », le projet doit, en lui-même, s'avérer conforme aux lois. Comme je l'ai mentionné à maintes reprises, cette vérification de la légalité constitue un exercice requérant des connaissances et des compétences juridiques et technologiques importantes et spécialisées. En principe, tout projet doit *d'abord* être légal, sans égard à la sensibilité des renseignements personnels utilisés, à la finalité de leur utilisation, à leur quantité, à leur répartition ou à leur support. En même temps, avant d'être en mesure de juger de la sensibilité des renseignements concernés, de la finalité de leur utilisation, de leur quantité, de leur répartition ou de leur support, encore faut-il colliger un minimum d'information permettant d'appliquer ces critères. Autrement dit, la possibilité de moduler l'ÉFVP en fonction des critères d'utilité, de quantité, de sensibilité, de répartition ou de support technologique pourrait n'avoir dans les faits aucun impact sur la quantité globale d'évaluation qui aurait à être produite, mais seulement sur l'envergure de chacun de ces exercices.

Supposons qu'un seul point de pourcentage de ces 8000 évaluations annuelles concernerait des projets qui requièrent de faire une ÉFVP exhaustive, il s'agirait tout de

[51] À cet égard, voir la liste en page 37.

même de 80 processus d'évaluation. Considérant, comme je l'ai déjà écrit en introduction de ce mémoire, que la transformation numérique est au cœur de la stratégie gouvernementale et de celles d'un grand nombre d'entreprises québécoises et canadiennes, cette seconde hypothèse paraît, encore une fois, très conservatrice (Jenkinson, 2021; Kabbaj, 2021; Raymond Chabot Grant Thornton, 2022; SCT, 2019). Dans son *Analyse d'impact réglementaire* sur le projet de loi 64, le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité (SRIDAIL)[52] partait plutôt de l'hypothèse que 3 % des entreprises privées devraient réaliser une ÉFVP pour l'évaluation de système informatique. (SAIRID, 2020, p. 20 et 24) En utilisant la même hypothèse que le SRIDAIL, nous obtenons une hypothèse de 26 490 ÉFVP sur une base annuelle, dont plus de 260 requerraient une analyse plus exhaustive, requérant l'évaluation des risques éthiques en plus des juridiques et technologiques[53]. Je rappelle que ces estimations ne tiennent pas compte des autres situations visées par une obligation de réaliser une ÉFVP. Je souligne également que celles-ci ne tiennent pas compte des ÉFVP qui pourraient devoir être révisées ponctuellement. Comme le souligne la CAI, l'ÉFVP « n'est efficace que si elle évolue de façon continue : elle doit être revue au besoin, tout au long de la vie du projet » (CAI, 2021, p. 6). En effet, considérant que le contexte dans lequel une solution informatique évolue et change constamment, au gré notamment des conditions socio-économiques, des modifications législatives et réglementaires, de l'innovation technologique et des changements politiques, l'ÉFVP devrait également être revue ponctuellement pour réévaluer les incidences de ces modifications sur la protection de la vie privée des personnes concernées. Ces processus de réévaluations s'ajouteraient donc aux nouvelles évaluations obligatoires.

[52] Connu à l'époque sous l'acronyme SAIRID, pour Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques.

[53] Je souligne par ailleurs que l'analyse du SRIDAIL ne tenait compte que des entreprises privées et ne considérait que le travail d'un avocat sur le dossier, à raison de 10 heures de travail pour ce dernier, sans tenir compte de l'évaluation des enjeux technologiques et des enjeux éthiques.

Bref, bien qu'il soit difficile d'estimer précisément combien d'ÉFVP seront réalisées dans les prochaines années et qu'il est impossible de prévoir l'envergure qu'elles auront toutes, il semble probable qu'il y en aura beaucoup, pour un grand nombre d'organisations et pour une variété importante de projets, certains impliquant des technologies complexes et émergentes pour lesquelles nous n'aurons que peu de recul. Pour ces dernières, une expertise de pointe encore plus rare et onéreuse — par exemple, en intelligence artificielle ou en cryptographie quantique — pourrait s'avérer essentielle. Ces constats remettent en question la faisabilité de la mesure en raison de la disponibilité des personnes ayant les compétences requises pour effectuer tous ces exercices. Peut-on toujours penser que l'obligation de réaliser une ÉFVP, appuyée sur l'hypothèse que les organisations seront à même de s'autoréguler par l'évaluation de la conformité aux lois et par l'évaluation des risques et des préjudices portés à la vie privée, permettra véritablement d'atteindre un niveau de protection acceptable de la vie privée? Si l'on veut que la réalisation des ÉFVP devienne un véritable levier dans l'amélioration globale de la protection de la vie privée et qu'elle remplisse ses objectifs, et que les organisations ne la réduisent pas à être une simple procédure bureaucratique, il est important que les ressources compétentes en la matière soient disponibles et qu'elles partagent toutes un objectif commun, soit celui de défendre la sécurité informationnelle du public et de respecter son droit à la vie privée.

3.4 *Conclusion*

Dans ce dernier chapitre, j'ai voulu mettre en lumière certains enjeux que soulève l'obligation de produire des ÉFVP pour tout système d'information ou prestations électroniques de services. C'est d'abord toute la question de la nature des risques et des préjudices portés à la vie privée qui a été soulevée. Ces caractéristiques m'ont mené à considérer que l'ÉFVP — minimalement celle réalisée pour des projets de plus grande envergure ou impliquant un plus nombre de personnes — ne pourrait faire l'économie d'une évaluation des enjeux plus proprement éthiques et d'une prise en compte du point de vue des personnes visées par le projet. Dans un deuxième temps, j'ai voulu esquisser les pourtours d'une réflexion portant sur le rôle de l'évaluateur lui-même, notamment quant aux

compétences requises pour tenir un tel exercice et sur la posture professionnelle à privilégier. C'est également la question de l'objectivité des processus d'évaluation et des potentiels conflits d'intérêts entre le rôle d'évaluateur et le processus de prise de décisions que j'ai voulu mettre en relief.

En guise de conclusion de ce chapitre, je me permettrais de faire montre d'un certain scepticisme devant l'applicabilité de l'obligation de réaliser des ÉFVP pour tout projet de système d'information ou de prestation électronique de services. D'abord, nous pouvons nous questionner sur la qualité moyenne des ÉFVP qui seront réalisées dans les prochaines années en raison des compétences spécialisées qui sont requises pour tenir dûment cet exercice. Si j'espère avoir au moins appuyé suffisamment sur un élément tout au long de ce mémoire, il s'agit de la complexité de la notion même de « protection de la vie privée ». L'évaluation des risques et des préjudices portés à celle-ci ne saurait vraisemblablement être résumée par une recette ou par une méthode pouvant être appliquée à la chaîne. Les ÉFVP souffriront peut-être d'un déficit de qualité en raison de la complexité de l'exercice. Il est pensable qu'elles soient reléguées la plupart du temps au statut d'exigence bureaucratique, considérées comme un mal nécessaire. Sur ce point, l'avenir seul nous le dira. Il faudra voir si la réalisation des ÉFVP apportera concrètement une conscientisation des organisations et des personnes concernées par leurs projets quant aux risques et des préjudices portés à la vie privée que le recours au numérique peut engendrer.

CONCLUSION GÉNÉRALE

À l'origine de ce travail de recherche se trouvait une intention pratique. Il s'agissait d'outiller les organisations qui allaient devoir produire des évaluations des facteurs relatifs à la vie privée (ÉFVP) pour la mise en œuvre d'un projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels. L'intention était de fournir des balises permettant de tenir un exercice qui serait au mieux protecteur de la vie privée. La question au fond était de savoir comment opérationnaliser la partie « évaluation des risques et des préjudices portés à la vie privée » qui est, selon ma lecture personnelle, au cœur de l'obligation de réaliser de tels processus d'évaluation. Je partais de l'hypothèse que la spécificité de l'ÉFVP réside dans l'exercice d'évaluer les risques et des préjudices portés à la vie privée plutôt que dans l'évaluation de la conformité juridique et de l'évaluation des mesures de sécurité de l'information. En considérant que la nouvelle obligation touchera un très grand nombre d'organisations, pour un grand nombre de projets potentiels, il semblait tout à fait utile de poser cette question dans un contexte de réflexion éthique. Si cette nouvelle obligation vise à améliorer la protection de la vie privée dans un contexte de transformation numérique des entreprises et des organismes publics, encore faut-il avoir une idée claire de ce que veut dire l'expression « protéger la vie privée ».

Dans le premier chapitre de mon mémoire, j'ai voulu mettre en lumière les principales caractéristiques de l'évaluation des risques et des préjudices. L'accent a été porté sur l'objectif présumé d'un tel processus, celui de protéger la vie privée des personnes. Il s'agissait en quelque sorte d'établir que la portion « évaluation des risques et préjudices portés à la vie privée » est la composante distinctive de l'ÉFVP. Une fois cette proposition faite, j'ai jugé bon de voir quelle serait la nature des risques et des préjudices qui devraient être considérés dans ce processus d'évaluation. Or, le domaine d'application d'un processus d'évaluation découle naturellement des objectifs que vise l'organisation par cette évaluation. Comme l'objectif de l'ÉFVP devrait logiquement être de protéger la vie privée des personnes concernées par le projet évalué, l'évaluateur devrait donc porter toute son attention sur cette

notion de « vie privée » et sur les moyens à mettre en place pour la protéger adéquatement. C'est pourquoi la question que j'ai ensuite posée fut celle de la nature des risques et des préjudices portés à la vie privée. En m'appuyant sur l'exemple des taxonomies proposées par Daniel Solove et Danielle Keats Citron, j'ai voulu mettre en relief le fait que les atteintes à la vie privée et les préjudices qui en découlent sont nombreux et fort variés.

Cette quantité et cette variété m'ont amené à me tourner vers la notion même de « vie privée » dans le second chapitre, l'objectif étant de voir comment répondre à la question « qu'est-ce que "protéger la vie privée"? » Cette recherche m'a mené à voir que les théoriciens ne s'entendent pas sur le sens à donner à cette réponse. En fait, il appert que cette notion est, dans les faits, multidimensionnelle, fortement liée au contexte duquel elle émerge et dans lequel elle est utilisée et qu'elle est essentiellement contestable, c'est-à-dire qu'il est dans sa nature même d'être constamment rediscutée et redéfinie. En conséquence, il semble que la réponse à la question « qu'est-ce que "protéger la vie privée"? » est elle aussi condamnée à évoluer au gré des changements sociaux et technologiques de la société à partir de laquelle elle se pose. En outre, la protection de la vie privée peut être perçue comme un outil permettant d'assurer la protection d'autres valeurs chères à nos sociétés démocratiques, notamment l'autonomie, l'identité, la liberté et la protection des personnes. En ce sens, les risques et les préjudices portés à la vie privée se confondent avec les risques éthiques. Ainsi, l'évaluation des risques et des préjudices portés à la vie privée est un processus analogue au fait d'évaluer les risques éthiques, comme le font par exemple les comités d'éthique de la recherche.

Le chapitre 3 visait à établir quelques liens entre l'évaluation des facteurs relatifs à la vie privée (ÉFVP) et les constats faits à propos de la protection de la vie privée. Mon intention a été d'esquisser certains enjeux éthiques propres à la réalisation des ÉFVP. J'ai voulu soulever le fait que, devant les considérations de rentabilité, d'efficacité et d'optimisation liées à la transformation numérique, l'objectivité et l'efficacité des futurs processus d'évaluation des risques et des préjudices qui seront réalisés peuvent être remises en question. Également, parce que la réalisation d'une ÉFVP fait appel à des compétences spécialisées à

la fois juridiques, technologiques et éthiques, il est possible de douter que l'obligation universelle de réaliser des ÉFVP pour un projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels donne lieu à des processus de qualité. Elle exige en outre qu'une certaine posture professionnelle soit adoptée par l'évaluateur. Ainsi, la réalisation de ces processus d'évaluation soulève également des questions en matière de professionnalisation de la fonction d'évaluateur des risques et des préjudices en matière de protection de la vie privée. La position occupée par ces personnes peut notamment engendrer certains conflits d'intérêts potentiels ou conflits de valeurs sur lesquels il sera pertinent de se pencher dans l'avenir.

Je disais donc au début de cette conclusion que mon objectif était d'abord pratique. Au fil de la lecture et de la recherche, un constat s'est rapidement dégagé : il n'est pas simple d'établir quels sont les risques et les préjudices portés à la vie privée parce qu'il n'est pas simple de définir d'abord ce qu'est la « vie privée ». Le sens de l'expression « protéger la vie privée » m'échappe encore, comme il semble échapper encore à la plupart des théoriciens par ailleurs, même si les idées se précisent un peu à chaque nouvelle lecture. J'en viens toutefois à douter de trouver une réponse unique, simple et pratique. La complexité de toute cette notion de « protection de la vie privée » permet d'entretenir un certain scepticisme quant à la possibilité des organisations à s'autoréguler adéquatement alors qu'elles auront à produire sous peu des évaluations des risques et des préjudices portés à la vie privée.

Ce tour d'horizon de la notion de risque et de préjudice portés à la vie privée est forcément incomplet. Comme je l'ai compris avec le texte de Mulligan, Koopman et Doty, la vie privée est un concept évolutif. Ses frontières et les mécanismes de protection qui lui sont accordés sont condamnés, en quelque sorte, à suivre l'évolution non seulement des technologies, mais également de la société. Les processus d'évaluation des risques et des préjudices portés à la vie privée se confondraient ainsi avec les processus d'évaluation éthique. Ainsi, l'obligation de réaliser une ÉFVP qui se voudrait véritablement protectrice de la vie privée — c'est-à-dire qui tient compte plus largement des risques éthiques — semble

rencontrer un double écueil : pratiquement d'abord, parce que les qualifications requises pour tenir un exercice juridiquement, technologiquement et éthiquement adéquat sont rares, tout comme le temps nécessaire pour faire ce genre d'exercice. Conceptuellement ensuite, pour des raisons déjà évoquées : par la nature même des risques et des préjudices portés à la vie privée, l'évaluation éthique des enjeux de protection de la vie privée se trouve en position de faiblesse par rapport aux impératifs économiques, commerciaux, d'innovation et d'optimisation des processus. L'analyse qui est produite dans le cadre d'une ÉFVP est délimitée au projet évalué, mais les enjeux et les impacts peuvent être globaux. Ils découlent en fait des effets cumulés du triplet mode de vie/transformation numérique/logique d'accumulation informationnelle. Ainsi, je me permets de faire écho aux propos de Mark Hunyadi qu'il tient dans son opuscule *La Tyrannie des modes de vie* (2015) et je pose la question suivante : au lieu de concourir à la protection de la vie privée, la production massive d'ÉFVP ne viendra-t-elle pas plutôt *blanchir éthiquement* le recours croissant au numérique? En servant de caution bureaucratique à la collecte, à l'utilisation et à la communication de quantité grandissante de renseignements personnels, toutes ces ÉFVP laisseront-elles graduellement la place à un mode de vie dans lequel la protection de la vie privée deviendrait impossible en raison de l'hégémonie numérique?

Cette dernière question est hypothétique, certes, et sans doute inutilement alarmiste. Sous réserve qu'elles soient le moindrement efficaces, toutes les mesures qui sont prises pour protéger la vie privée ont leur importance. Cela étant dit, quelle suite donner à tout ce qui a été dit jusqu'ici? Considérant l'aspect hautement contextuel et évolutif de ce qui est une atteinte à la vie privée, quel conseil donner à une organisation qui se voudrait véritablement protectrice de la vie privée? À l'instar des appels à la frugalité et à la décroissance lancés par les environnementalistes, notamment par le groupe de réflexion *Shift Project* (2018) qui a popularisé l'expression « sobriété numérique », il semblerait intéressant d'explorer l'idée d'un principe de frugalité ou de sobriété informationnelle. Il pourrait être intéressant d'évoquer et de poursuivre ici avec la comparaison maintes fois énoncée entre le pétrole et la donnée. Tout comme pour le pétrole, c'est la grande quantité utilisée de ce nouvel « or noir » qui revêt un aspect potentiellement préjudiciable. Plus nous dépendons et brûlons des

combustibles fossiles et plus l'environnement en souffre en raison de l'accumulation de gaz à effet de serre. De façon analogue, plus nous collectons, générons, accumulons, utilisons et communiquons des renseignements personnels, plus les risques d'engendrer des préjudices s'accroissent. Pour reprendre une expression du domaine de la cybersécurité, plus des renseignements personnels sont à disposition, plus les surfaces potentielles d'attaque se multiplient.

Or, comme Neil Richards, Carissa Véliz et de nombreux autres auteurs le soulignent, la protection de la vie privée consiste, en partie du moins, à rétablir l'équilibre du pouvoir entre les citoyens et consommateurs et les personnes ou les organisations qui détiennent des renseignements sur eux. Cela étant dit, comme nous sommes à même de le constater au fil de l'actualité internationale, les démocraties peuvent s'étioler et sombrer dans l'autoritarisme. De nouvelles sources de vulnérabilités surgissent avec les nouvelles technologies, ou d'anciennes vulnérabilités sont exacerbées par la démocratisation de leur usage. Le visage des minorités et des personnes vulnérables se transforme. Le droit change et cette évolution ne va pas toujours dans un sens avantageux pour tous. Le renversement du jugement Roe v. Wade le démontre bien : une information anodine en apparence (par exemple, les données de géolocalisation) peut revêtir soudainement un caractère éminemment sensible en raison d'un contexte juridique fluctuant. En l'occurrence, les données de géolocalisation démontrant une visite dans une clinique prodiguant des services d'avortement deviennent potentiellement préjudiciables si une telle visite a lieu dans un état où l'avortement est criminalisé. Mais, alors que le niveau de protection de la vie privée dont nous jouissons peut fondre du jour au lendemain, les renseignements ne disparaissent pas toujours aussi facilement. L'insouciance que nous avions la veille à fournir nos renseignements personnels peut devenir la cause de nos angoisses. Ignorer cette réalité, c'est faire en quelque sorte le pari que les réalités socioéconomiques, politiques et juridiques de demain seront identiques à celles d'aujourd'hui. Protéger la vie privée des personnes consisterait peut-être plutôt à limiter ou interdire tout simplement la collecte, l'utilisation et la communication des renseignements portant sur une personne.

Entre-temps, pour revenir aux termes de la réflexion d'Hunyadi, le mode de vie axé sur le recours au numérique se renforce sous l'effet cumulé des innovations et du déploiement des différentes technologies. Ultimement, la responsabilité de tenir compte des risques et des préjudices portés à la vie privée devrait peut-être moins reposer sur les organisations que sur une discussion tenue par la société dans son ensemble. Une prise en charge véritable des risques et des préjudices portés à la vie privée repose sans doute moins sur l'évaluation *à la pièce* de chaque projet individuel que sur une réflexion globale et collective concernant la place du numérique dans nos existences. Pour reprendre les conclusions d'Hunyadi, la protection de la vie privée bénéficierait sans doute d'une réappropriation collective de la question du mode de vie imposé par la transformation numérique. Or, il paraît hautement improbable qu'une telle remise en question ait lieu avant longtemps au sein de la société québécoise, considérant la forte impulsion mondiale vers le numérique, la course à l'innovation et — il faut savoir le reconnaître — les bénéfices importants et, surtout, tangibles découlant des outils technologiques.

Faut-il le rappeler toutefois, le risque accompagne généralement l'opportunité. Il en forme, en quelque sorte, son versant négatif. Or, l'opportunité peut justifier la prise de risque si elle paraît bénéfique et si elle s'avère éthiquement justifiée. Ainsi, l'interdiction pure et simple d'utiliser des renseignements personnels semblerait être une solution à la fois radicale, trop simpliste et, dans bien des cas, préjudiciable (par exemple, en ce qui concernerait la recherche médicale). L'idée de limitation paraît plus raisonnable et elle me ramène à l'idée de frugalité ou de sobriété informationnelle. Pour *le Petit Robert,* la notion de « frugalité » renvoie à ce qui est frugal. Elle signifie ce « qui consiste en aliments simples, peu recherchés, peu abondants », « qui se contente d'une nourriture simple » et sobriété, au « comportement d'une personne, d'un animal qui boit et mange avec modération ». L'attitude à privilégier face au choix d'avoir recours au numérique et aux renseignements personnels devrait peut-être être empreinte de modération et de réserve, c'est-à-dire de privilégier un recours frugal et raisonnable aux données concernant les personnes. Une telle attitude renvoie à l'idée du principe de nécessité qui existe déjà dans la Loi sur l'accès. Il s'agirait d'en revenir au fait de collecter, d'utiliser et de communiquer le nécessaire et ce qui est véritablement utile. Ce

serait prôner une utilisation modérée et, surtout, judicieuse des renseignements personnels. L'idée ne serait pas d'en interdire la collecte ou l'utilisation, mais plutôt de collecter et d'utiliser « mieux ». Cette idée renverrait toutefois à un tout autre débat, celui de définir ce qui est *véritablement utile*. Cela constituerait en soi un important chantier de réflexion. L'évaluateur chargé de procéder à l'ÉFVP devrait tout de même avoir toute la latitude pour dire non à un projet jugé non nécessaire, sans égard aux bénéfices attendus de l'organisation qui l'emploie. Néanmoins, tout comme les environnementalistes ont peiné à être entendus face aux impératifs de productivité dans les premiers temps de leur combat pour la protection de l'environnement, il est permis de douter qu'un appel lancé à la frugalité informationnelle le soit plus facilement dans le contexte actuel de transformation numérique.

RÉFÉRENCES BIBLIOGRAPHIQUES

AFP. (2022a, 24 mai). *Des démocrates demandent à Google de protéger les données des femmes voulant avorter*. Le Journal de Montréal. https://www.journaldemontreal.com/2022/05/24/des-democrates-demandent-a-google-de-proteger-les-donnees-des-femmes-voulant-avorter

AFP. (2022b, 26 juin). *Les données personnelles en jeu après l'abolition du droit à l'avortement aux États-Unis*. Radio-Canada.ca. https://ici.radio-canada.ca/nouvelle/1893915/donnees-personnelles-droit-avortement-etats-unis-facebook-google-application

AFP. (2022c, 1er juillet). *Google supprimera les données sur les visites aux cliniques d'avortement*. La Presse. https://www.lapresse.ca/affaires/techno/2022-07-01/google-supprimera-les-donnees-sur-les-visites-aux-cliniques-d-avortement.php

Allen, A. (2011). Unpopular Privacy: What Must We Hide? Oxford University Press Usa.

ARC. (2022, 11 mai). *Évaluation des facteurs relatifs à la vie privée*. Agence du revenu du Canada. https://www.canada.ca/fr/agence-revenu/services/a-propos-agence-revenu-canada-arc/protection-vos-renseignements-personnels/evaluation-facteurs-relatifs-a-vie-privee.html

Armus, T. (2017, 22 novembre). *Facebook can tell whether you're gay based on a few « likes, » study says*. NBC News. https://www.nbcnews.com/feature/nbc-out/facebook-can-tell-if-you-re-gay-based-few-likes-n823416

Assemblée générale des Nations unies. *Déclaration universelle des droits de l'homme*. https://www.un.org/fr/universal-declaration-human-rights/index.html

ATN. (2021a, 15 juin). *Portrait des usages du numérique dans les écoles québécoises*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/autres-publications/2021-06-portrait-des-usages-du-numerique-dans-les-ecoles-quebecoises

ATN. (2021b, 29 septembre). *Maison intelligente : le portrait québécois*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2021-09-maison-intelligente-le-portrait-quebecois

ATN. (2021c, 21 novembre). *Services bancaires en ligne*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2021-10-services-bancaires-en-ligne

ATN. (2021d, 9 décembre). *Les aînés connectés au Québec*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2021-12-les-aines-connectes-au-quebec

ATN. (2022a, 2 mars). *La famille numérique*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-03-la-famille-numerique

ATN. (2022b, 30 mars). *Le commerce électronique*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-03-le-commerce-electronique

ATN. (2022c, 27 avril). *Les services gouvernementaux en ligne et l'identité numérique*. [Rapport d'enquête]. Académie de la transformation numérique. https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-04-les-services-gouvernementaux-en-ligne-et-lidentite-numerique

Austin, L. M. (2014). Enough About Me: Why Privacy is About Power, not Consent (or Harm). Dans A. Sarat (dir.), *A World without Privacy: What Law Can and Should Do?* (p. 131-189). Cambridge University Press.

Barth, S. et de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Benoit, F. (2019). *The Valley : une histoire politique de la Silicon Valley.* Les Arènes.

Benyekhlef, K. et Déziel, P.-L. (2018). *Le droit à la vie privée en droit québécois et canadien*. Éditions Yvon Blais.

Bizet, T. (2017). L'ambition individualiste de l'autodétermination informationnelle. *Revue internationale de droit des données et du numérique*, *3*(0), 49-60.

Borgès Da Silva, R. (2013). Taxonomie et typologie : est-ce vraiment des synonymes ? *Santé Publique*, *25*(5), 633. https://doi.org/10.3917/spub.135.0633

Bracy, J. (2022, 3 mai). Leaked Roe v. Wade opinion sparks right-to-privacy concerns. *The Privacy Advisor*. https://iapp.org/news/a/leaked-roe-v-wade-opinion-sparks-right-to-privacy-concerns/

Breton, P. (1997). *L'utopie de la communication : le mythe du « village planétaire »*. La Découverte.

CAI. (2016). *Rétablir l'équilibre*. [Rapport quinquennal]. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf

CAI. (2020, 4 mai). *Pandémie, vie privée et protection des renseignements personnels*. [Document de réflexion]. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/documents/CAI_document-reflexion_PRP_COVID-19_FR.pdf

CAI. (2021, mars). *Guide d'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée*. [Guide pratique]. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf

CAI. (2022a, 28 janvier). *Biométrie*. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/biometrie/

CAI. (2022b, 17 février). *Loi sur la protection des renseignements personnels dans le secteur privé - version administrative*. [Document de travail]. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/documents/CAI_Loi_prive_version_administrative.pdf

CAI. (2022c, 17 février). *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels - version administrative*. [Document de travail]. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/documents/CAI_Loi_acces_version_administrative.pdf

CAI. (s. d.). *Anonymisation*. Commission d'accès à l'information. https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/anonymisation/

Cavoukian, A. (2011, janvier). *The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

CDPDJ. (2020, octobre). *Mémoire à la Commission des institutions de l'Assemblée nationale - Projet de loi no 64, Loi modernisant les dispositions législatives en matière de protection des renseignements personnels*. [Mémoire]. Commission des droits de la personne et de la protection de la jeunesse. https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf

CEFRIO. (2019). *Portrait numérique des foyers québécois* (Volume 10-Numéro 4). [Rapport d'enquête] https://numerique.banq.qc.ca/patrimoine/details/52327/4146270

CEST. (2020a, novembre). *L'Internet des objets, la vie privée et la surveillance*. [Avis]. Commission de l'éthique en science et en technologie. https://www.ethique.gouv.qc.ca/media/1338/cest_ia_cai_2020.pdf

CEST. (2020b, mai). *Réponse au document de consultation sur l'intelligence artificielle de la Commission d'accès à l'information du Québec*. Commission de l'éthique en science et en technologie. https://www.ethique.gouv.qc.ca/media/1338/cest_ia_cai_2020.pdf

Chandran, R. (2021, 17 août). *Afghans scramble to delete digital history, evade biometrics*. Reuters. https://www.reuters.com/article/afghanistan-tech-conflict-idUSL8N2PO1FH

Charte canadienne des droits et libertés. Partie I de la Loi constitutionnelle de 1982, annexe B de la Loi de 1982 sur le Canada. RU. (1982). c. 11. http://laws.justice.gc.ca/fra/Const/page-15.html

Charte des droits et libertés de la personne. RLRQ c. C -12. http://legisquebec.gouv.qc.ca/fr/showdoc/cs/C-12

Chassigneux, C. (2020, 11 décembre). *Fédération des caisses Desjardins du Québec* 1020846-S (Commission d'accès à l'information du Québec). https://decisions.cai.gouv.qc.ca/cai/ss/fr/item/490078/index.do

Clarke, R. (1997). *Privacy Introduction and Definitions*. http://www.rogerclarke.com/DV/Intro.html#PrivProt

Clarke, R. (2009). Privacy impact assessment : Its origins and development. *Computer Law & Security Review*, *25*(2), 123-135. https://doi.org/10.1016/j.clsr.2009.02.002

Clarke, R. (2021, 26 mai). Roger Clarke's Dataveillance and Information Privacy Home-Page. http://www.rogerclarke.com/DV/

CNIL. (2019, 22 octobre). *Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)*. Commission Nationale de l'Informatique et des Libertés. https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Code des professions. RLRQ, c. chapitre C-26. https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-26

Cofone, I. N. (2019). Nothing to hide, but something to lose. *University of Toronto Law Journal*, *70*(1), 64-90. https://doi.org/10.3138/utlj.2018-0118

Cofone, I. et Robertson, A. (2018). Privacy Harms. *Hastings Law Journal*, *69*(4), 1039-1098.

Cohen, J. E. (2013). What Privacy is for? *Harvard Law Review*, *126*(7), 1904-1933.

Comeau, P.-A. (2012). Protection des renseignements personnels. Dans *Le Dictionnaire encyclopédique de l'administration publique* (p. 4). École nationale d'administration publique. Récupéré le 20 septembre 2021 de http://www.dictionnaire.enap.ca/Dictionnaire/1/Dictionnaire.enap

COMEST. (2005, mars). *Le Principe de précaution*. [Avis]. Commission mondiale d'éthique des connaissances scientifiques et des technologies. https://unesdoc.unesco.org/ark:/48223/pf0000139578_fre

Commission de la culture et de l'éducation. (2020). *Mandat d'initiative portant sur l'avenir des médias d'information*. [Mémoire]. Assemblée nationale. http://assnat.qc.ca/fr/travaux-parlementaires/commissions/cce/mandats/Mandat-40735/index.html

Couldry, N. et Mejias, U. A. (2019a). Datafication. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1428

Couldry, N. et Mejias, U. A. (2019b). Making data colonialism liveable: how might data's social order be regulated? *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1411

Couldry, N. et Mejias, U. A. (2020). *The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism*. Standford University Press.

Cox, J. (2022, 17 mai). Data Marketplace Selling Info About Who Uses Period Tracking Apps. *Vice*. https://www.vice.com/en/article/v7d9zd/data-marketplace-selling-clue-period-tracking-data

CPVPC. (2011, 13 octobre). *Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée*. [Guide]. Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/gd_exp_202003/

CPVPC. (2021, 3 février). *Conclusions en vertu de la LPRPDE no 2021-001 : Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta*. [Rapport d'enquête]. Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/

De Grosbois, P. (2018). *Les batailles d'Internet : Assauts et résistances à l'ère du capitalisme numérique*. Écosociété.

DeCew, J. (2018, 18 janvier). Privacy. Dans *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/spr2018/entries/privacy/

Déclaration de Montréal - pour un développement responsable de l'intelligence artificielle. (2018). https://www.declarationmontreal-iaresponsable.com/

Department of Justice. (2014, 16 juin). *E-Government Act of 2002*. [Site web gouvernemental]. The United States Department of Justice. https://www.justice.gov/opcl/e-government-act-2002

Déziel, P.-L. (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*, *30*(3), 829-850. https://www.lescpi.ca/s/3745

Dionne, B. (2006, 25 août). *Développement de scénarios d'analyse de risques en matière de protection des renseignements personnels (PRP) intégrés à la méthodologie Méhari*. [Guide]. Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information. https://numerique.banq.qc.ca/patrimoine/details/52327/45371

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. OPOCE. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A31995L0046

Directive sur l'évaluation des facteurs relatifs à la vie privée. (2010, 29 mars). Secrétariat du Conseil du trésor du Canada. https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308#appC

Duby, G. et Ariès, P. (1999). *Histoire de la vie privée* ([Éd. rev. et complétée].). Éditions du Seuil.

Duhigg, C. (2012, 16 février). How Companies Learn Your Secrets. *The New York Times*, section Magazine. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

EDPB et AEPD. (2021, mai). *10 misunderstanding related to anonymisation*. [Guide]. European Data Protection Board. https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf

FCC. (2022, 22 mai). The environmental cost of email. *Fight Climate Change*. https://fightclimatechange.earth/2022/05/22/the-environmental-cost-of-email/

Finn, R. L., Wright, D. et Friedewald, M. (2013). Seven Types of Privacy. Dans S. Gutwirth, R. Leenes, P. de Hert et Y. Poullet (dir.), *European Data Protection : Coming of Age* (p. 3-32). Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_1

Floridi, L. (2017). Group Privacy: A Defence and an Interpretation. Dans L. Taylor, L. Floridi et B. van der Sloot (dir.), *Group Privacy* (p. 83-100). Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_5

Gallie, W. B. (1956). Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, *56*(1), 167-198. https://doi.org/10.1093/aristotelian/56.1.167

Gallie, W. B. (2014). Les concepts essentiellement contestés. *Philosophie*, *N° 122* (3), 9. https://doi.org/10.3917/philo.122.0009

Gautrais, V. et Aubin, N. (2022, mars). *Modèle d'évaluation des facteurs relatifs à la circulation des données - Instrument de protection de la vie privée et des droits et libertés dans le développement et l'usage de l'intelligence artificielle*. [Rapport de recherche]. Chaire L.R. Wilson. http://chairelrwilson.openum.ca/files/sites/36/2022/03/Modele_IA_Version_0.1.pdf

Gouvernement du Canada. (2018). *Énoncé de politique des trois conseils, éthique de la recherche avec des êtres humains.* [Document d'encadrement]. http://publications.gc.ca/collections/collection_2019/irsc-cihr/RR4-2-2019-fra.pdf

Gouvernement du Canada. (2020). *L'avenir des communications au Canada : Le temps d'agir : rapport final.* [Rapport]. Ministère de l'Industrie. http://www.deslibris.ca/ID/10103213

Gouvernement du Canada. (2022, 31 mars). *Recherche et statistique sur la PME*. [Rapport d'enquête]. Innovation, Sciences et Développement économique Canada. http://www.ic.gc.ca/eic/site/061.nsf/fra/accueil

Gouvernement du Québec. (2021, 17 décembre). *Contexte - Stratégie de transformation numérique gouvernementale 2019-2023*. [Stratégie gouvernementale]. Quebec.ca. https://www.quebec.ca/gouvernement/politiques-orientations/vitrine-numeriqc/strategie-numerique/a-propos

Gouvernement du Québec. (2022, 20 avril). *Stratégies et politiques / Offensive de transformation numérique*. [Stratégie gouvernementale]. Ministère de l'Économie et de l'Innovation. https://www.economie.gouv.qc.ca/bibliotheques/strategies/offensive-de-transformation-numerique/

Groupe de travail « article 29 ». (2017, 17 avril). *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679*. [Lignes directrices]. Groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel. https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

Gutwirth, S., Friedewald, M., Wright, D., Mordini, E. et Venier, S. (2011, 23 mars). *Legal, social, economic and ethical conceptualisations of privacy and data protection*. [Rapport de recherche]. Seventh Framework Programme. http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf

Hansson, S. O. (2004). Philosophical Perspectives on Risk. *Techné: Research in Philosophy and Technology*, *8*(1), 10-35. https://doi.org/10.5840/techne2004818

Harari, Y. N. (2017). *Homo deus : une brève histoire de l'avenir*. Albin Michel.

Hu, M. (2021, 2 septembre). *Afghanistan : quand la protection des données biométriques devient une question de vie ou de mort*. The Conversation. http://theconversation.com/afghanistan-quand-la-protection-des-donnees-biometriques-devient-une-question-de-vie-ou-de-mort-167124

Hunyadi, M. (2015). *La tyrannie des modes de vie : sur le paradoxe moral de notre temps*. Le Bord de l'eau.

ICO. (2022, 23 mai). *ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted*. [Fil d'actualité]. Information Commissioner's Office. ICO. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

IFCC. (2020, 27 août). *Résumés des évaluations des facteurs relatifs à la vie privée* [Site web]. Immigration, Réfugiés et Citoyenneté Canada. https://www.canada.ca/fr/immigration-refugies-citoyennete/organisation/transparence/acces-information-protection/evaluation-facteurs-relatifs-vie-privee.html

International Electrotechnical Commission. (2013, novembre). *IEC 60050 - International Electrotechnical Vocabulary - Details for IEV number 351-57-03: « risk »*. International Electrotechnical Vocabulary. https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-57-03

Organisation internationale de normalisation. (2018). *Management du risque — Lignes directrices*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v 1:fr

Organisation internationale de normalisation. (2017). *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'étude d'impacts sur la vie privée* (ISO/IEC 29134:2017(F)). https://www.iso.org/fr/standard/62289.html

ISQ. (2021a, 19 mai). *Nombre d'entreprises actives au Québec en décembre 2020*. [Rapport d'enquête]. Institut de la Statistique du Québec. https://statistique.quebec.ca/fr/document/nombre-entreprises-actives-quebec

ISQ. (2021b, 30 juin). *Évolution de statistiques clés de la culture et des communications, Québec*. [Rapport d'enquête]. Institut de la Statistique du Québec. https://statistique.quebec.ca/fr/document/evolution-de-statistiques-cles-de-la-culture-et-des-communications-quebec/tableau/evolution-de-statistiques-cles-de-la-culture-et-des-communications-quebec

ISQ. (2022, 24 mai). *L'utilisation d'Internet et des technologies dans les entreprises québécoises en 2020*. [Rapport d'enquête]. Institut de la Statistique du Québec. https://statistique.quebec.ca/fr/document/utilisation-internet-et-technologies-entreprises-quebecoises-2020

Jarvis Thomson, J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *4*(4), 295-314. https://www.jstor.org/stable/2265075

Jenkinson, D. (2021, 7 juin). *Les cadres canadiens adoptent une approche « acheter ou développer » à l'égard de l'investissement stratégique*. Ernst & Young. https://www.ey.com/fr_ca/ccb/canadian-executives-take-buy-vs-build-approach-to-strategic-investing

Johnson, B. (2010, 11 janvier). *Privacy no longer a social norm, says Facebook founder*. The Guardian. https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Johnston, A. (2020). Individuation : Re-Imagining Data Privacy Laws to Protect Against Digital Harms. *Brussels Privacy Hub Working Paper*, *6*(24), 22.

Kabbaj, R. (2021, 25 septembre). *Le train de la transformation numérique est désormais en marche*. Le Devoir. https://www.ledevoir.com/economie/634506/transformation-numerique-le-train-est-desormais-en-marche

Kasper, D. V. S. (2005). The Evolution (or Devolution) of Privacy. *Sociological Forum*, *20*(1), 69-92. https://doi.org/10.1007/s11206-005-1898-z

Kermisch, C. (2012). Vers une définition multidimensionnelle du risque. *VertigO*, *12*(2), 15. https://doi.org/10.4000/vertigo.12214

Koivisto, R. et Douglas, D. (2015, juin). *Principles and Approaches in Ethics Assessment: Ethics and Risk*. (Délivrable 1.1). [Rapport de recherche]. SATORI. https://satoriproject.eu/media/1.h-Ethics-and-Risk1.pdf

Kontargyris, X. (2020, 11 octobre). *7 principes pour le Privacy by Design - Renforcer le respect de la protection des données*. More Than Digital. https://morethandigital.info/fr/7-principes-pour-le-privacy-by-design-renforcer-le-respect-de-la-protection-des-donnees/

Koops, B.-J., Newell, B. C., Timan, T., Chokrevski, T. et Galic, M. (2017). A Typology of Privacy. *Journal of International Law*, *38*, 483-575. https://scholarship.law.upenn.edu/jil/vol38/iss2/4

Kröger, J. L., Miceli, M. et Müller, F. (2021). How Data Can Be Used Against People: A Classification of Personal Data Misuses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3887097

Lacroix, A., Marchildon, A., & Bégin, L. (2017). *Former à l'éthique en organisation : Une approche pragmatiste*. Presses de l'Université du Québec.

Lafontaine, C. (2004*). L'empire cybernétique : des machines à penser à la pensée machine*. Seuil.

Legault, G. A. (2004). *Professionnalisme et délibération éthique : manuel d'aide à la décision responsable*. Presses de l'Université du Québec.

LINC-CNIL. (2019, janvier). *La Forme des choix - Données personnelles, design et frictions dérisables* (6). Commission Nationale de l'Informatique et des Libertés. https://linc.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf

Loi, M. et Christen, M. (2020). Two Concepts of Group Privacy. *Philosophy & Technology*, *33*(2), 207-224. https://doi.org/10.1007/s13347-019-00351-0

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels. LQ. (2021). c. 25 http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25F.PDF

Louisot, J.-P. (2014). *Gestion des risques* (2e éd). Afnor éd. https://international-scholarvox-com.ezproxy.uqar.ca/book/88823559

Macnish, K. N. J. (2019). Introduction to Privacy. Dans C. Veliz (Ed.), *Data, Privacy and the Individual* IE University Press. https://research.utwente.nl/files/157795468/CGC_Data_Privacy_The_Individual_Paper_1._Introduction_to_Privacy.pdf

Malboeuf, M.-C. (2022, 7 mai). *Données de géolocalisation, on vous suit !* La Presse. https://www.lapresse.ca/affaires/2022-05-07/donnees-de-geolocalisation-on-vous-suit.php

Matsakis, L. (2022, 11 mai). *Privacy groups warn about data-tracking if Roe is overturned*. NBC News. https://www.nbcnews.com/tech/roe-v-wade-overturned-online-privacy-data-tracking-risk-rcna27492

McAfee. (2009). *The Carbon Footprint of Email Spam Report*. McAffee. https://www.siskinds.com/wp-content/uploads/carbonfootprint_12pg_web_rev_na-1.pdf

Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, *39*(3), 411-428. https://doi.org/10.1111/j.1467-9833.2008.00433.x

Moore, A. D. (2003). Privacy: Its Meaning and Value. *American Philosophical Quarterly*, *40*(3), 14. https://philpapers.org/rec/MOOPIM-2

Mulligan, D. K., Koopman, C. et Doty, N. (2016). Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118. https://doi.org/10.1098/rsta.2016.0118

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 41. https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Olson, P. (2022, 4 mai). *Online Privacy Becomes Critical If Roe v. Wade Is Overturned*. Washington Post. https://www.washingtonpost.com/business/online-privacy-becomes-critical-if-roe-v-wade-is-overturned/2022/05/04/ac183740-cb96-11ec-b7ee-74f09d827ca6_story.html

OQLF. (2003). Prestation électronique de services. Dans *Le Grand dictionnaire terminologique*. Récupéré le 24 mai 2022 de https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8359224

OQLF. (2004). Système d'information. Dans *Le Grand dictionnaire terminologique*. Récupéré le 24 mai 2022 de https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8358435

OQLF. (2020a). Biométrie. Dans *Le Grand dictionnaire terminologique*. Récupéré le 27 avril 2022 de https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8370889

OQLF. (2020b). Transformation numérique. Dans *Le Grand dictionnaire terminologique*. Récupéré le 13 mai 2022 de https://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26558201

OQLF. (2020c, 17 avril). Risque. Dans *Le Grand dictionnaire terminologique*. Récupéré le 16 janvier 2022 de https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_risque/risque.html

Ouellet, M. (2016). *La révolution culturelle du capital : le capitalisme cybernétique dans la société globale de l'information*. Écosociété.

Ouellet, M. (2021). Pour une théorie critique de la gouvernance algorithmique et de l'intelligence artificielle. *Tic & société*, (Vol. 15, N° 1 | 1er semestre), 9-40. https://doi.org/10.4000/ticetsociete.5603

Perron, S. (2020). La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique. *Lex Electronica*, *26*(2), 36-47. https://www.lex-electronica.org/en/s/1959

Poulsen, F. E. (2019a, 25 octobre). Towards a history of privacy: conceptual and methodological considerations [Billet]. *Centre for Privacy Studies*. https://privacy.hypotheses.org/189

Poulsen, F. E. (2019b, 7 décembre). Traduire privacy : Vie privée ou sphère privée ? [Billet]. *Centre for Privacy Studies*. https://privacy.hypotheses.org/427

Privé. (s. d.). Dans *Le Petit Robert* (2007e éd., p. 2026). Le Robert.

R. c. Jarvis. (2019, 14 février). [2019] 1 RCS 488 (Cour suprême du Canada). https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/17515/index.do?site_preference=normal

Rawls, J. (2009). *Théorie de la justice*. Points.

Raymond Chabot Grant Thornton. (2022, avril). *Sondage express sur la transformation numérique des entreprises québécoises*, 18. https://www.rcgt.com/app/uploads/2022/04/sondage_2022_maturite_numerique_pme_rcgt_som.pdf

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels. RLRQ, c. c. A-2.1, r. 2. http://legisquebec.gouv.qc.ca/fr/ShowDoc/cr/A-2.1,%20r.%202/

Règlement (UE) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE c. 2016/679. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

Rey, B. (2012). La privacy à l'ère du numérique. *Terminal*, (110), 91-103. https://doi.org/10.4000/terminal.1242

Richards, N. (2022). *Why privacy matters*. Oxford University Press.

Richards, N. et Hartzog, W. (2019). The Pathologies of Digital Consent. *Washington University Law Review*, *96*, 43. https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview

Risque. (s. d.). Dans *Le Petit Robert* (2007e éd., p. 2257). Le Robert.

Roe v. Wade. (1973, 22 janvier). 410 U.S. 70-18 U.S. Supreme Court 113.

Rossi, J. (2020). *Protection des données personnelles et droits à la vie privée : enquête sur la notion controversée de « données à caractère personnel »* [Université de technologie de Compiègne]. https://tel.archives-ouvertes.fr/tel-03155480

Roussel, D. et Bistodeau, D. (2009). *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics, version 1,1*. Ministère du conseil exécutif du Québec. http://collections.banq.qc.ca/ark:/52327/1821607

Sadin, É. (2016). *La silicolonisation du monde : l'irrésistible expansion du libéralisme numérique*. Éditions l'Échappée.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, *6*(1), 205395171882054. https://doi.org/10.1177/2053951718820549

SAIRID. (2020, 30 juillet). *Analyse d'impact règlementaire - Projet de loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/AIR_PL_PRP.pdf?1597071464

Salvat, C. (2020). *L'utilitarisme*. La Découverte.

Santé Canada. (2020, 29 octobre). *Alerte COVID : Évaluation de la protection de la vie privée de l'application de notification d'exposition à la COVID-19*. Gouvernement du Canada. https://www.canada.ca/fr/sante-publique/services/maladies/maladie-coronavirus-covid-19/alerte-covid/politique-confidentialite/evaluation.html

Schwab, K. (2017, 25 octobre). *La Quatrième révolution industrielle : ce qu'elle implique et comment y faire face*. Forum Économique Mondial. https://fr.weforum.org/agenda/2017/10/la-quatrieme-revolution-industrielle-ce-qu-elle-implique-et-comment-y-faire-face/

SCT. (2019). *Stratégie de transformation numérique gouvernementale 2019-2023 : mesures clés*. [Stratégie gouvernementale]. Secrétariat du Conseil du trésor. http://collections.banq.qc.ca/ark:/52327/4009307

SCT-TBC. (2010, 1er avril). *Directive sur l'évaluation des facteurs relatifs à la vie privée*. Secrétariat du Conseil du Trésor du Canada. https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308

Skinner-Thompson, S. (2017). *Performative Privacy*. University of California, Davis Law Review, 50, 1673-1739. https://scholar.law.colorado.edu/articles/403

Skinner-Thompson, S. (2022, 15 juin). *Privacy isn't in the Constitution—but it's everywhere in constitutional law*. The Conversation. http://theconversation.com/privacy-isnt-in-the-constitution-but-its-everywhere-in-constitutional-law-183204

Solove, D. J. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, *53*, 1393.

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*, Pages 1087-1156.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Solove, D. J. (2007). « I've Got Nothing to Hide » and Other Misunderstandings of Privacy. *George Washington University Law School*, 29.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Solove, D. J. (2020). The Myth of the Privacy Paradox. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3536265

Solove, D. J. (2022). The Limitations of Privacy Rights. *SSRN Electronic Journal*, 50. https://doi.org/10.2139/ssrn.4024790

Solove, D. J. et Citron, D. (2021). Privacy Harms. *SSRN Electronic Journal*, 55. https://doi.org/10.2139/ssrn.3782222

Sprenger, P. (1999, 26 janvier). *Sun on Privacy: « Get Over It »*. Wired. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

SRIDAIL. (2021, 3 décembre). *Mission et mandats*. [Site web gouvernemental]. Quebec.ca. https://www.quebec.ca/gouvernement/ministeres-et-organismes/institutions-democratique-acces-information-laicite/mission-mandats

SRIDAIL. (2022, 8 avril). *Évaluation des facteurs relatifs à la vie privée*. [Site web gouvernemental]. Quebec.ca. https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/evaluation-facteurs-relatifs-vie-privee

Statistique Canada. (2021, 5 février). *Magasinage en ligne pendant la pandémie de COVID-19*. https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2020088-fra.htm

Sullivan, B. (2022, 5 mai). *Could overturning Roe v. Wade have implications beyond abortion?* NPR. https://www.npr.org/2022/05/05/1096732347/roe-v-wade-implications-beyond-abortion

Taylor, L. et Floridi, L. (2017). *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer.

TECHNOcompétences. (2021). *Diagnostic Sectoriel 2021-2024 - Portrait de la main d'œuvre dans le secteur des technologies de l'information et des communications (TIC) au Québec*. TECHNOcompétences. https://www.technocompetences.qc.ca/wp-content/uploads/2021/08/TC_Diagnostic-Sectoriel_Page_LowRes_20200802.pdf

The Shift Project. (2018, octobre). *Pour une sobriété numérique*. The Shift Project. https://theshiftproject.org/article/pour-une-sobriete-numerique-rapport-shift/

Turner, F. (2006). *From counterculture to cyberculture : Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press.

UNESCO. (2022). *Recommandation sur l'éthique de l'intelligence artificielle*. Organisation des Nations Unies pour l'éducation, la science et la culture.

Véliz, C. (2019, 22 octobre). Privacy is a collective concern. *New Statesman*. https://www.newstatesman.com/science-tech/2019/10/privacy-collective-concern

Véliz, C. (2020). Priv*acy is Power: Why and How You Should Take Back Control of Your Data*. Penguin Random House UK.

Véliz, C. (2021). Privacy and digital ethics after the pandemic. *Nature Electronics*, *4*(1), 10-11. https://doi.org/10.1038/s41928-020-00536-y

Vie. (s. d.). Dans *Le Petit Robert* (2007e éd., p. 2709-2710). Le Robert.

Warren, S. D. et Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.

Westin, A. F. (1960). *Privacy and Freedom*. Athenum.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, *113*(6), 1153-1221.

Wittgenstein, L. et Rigal, É. (2014). *Recherches philosophiques* (F. Dastur, M. Élie, J.-L. Gautero, D. Janicaud et É. Rigal, trad.). Gallimard.

Zarsky, T. Z. (2015). The Privacy-Innovation Conundrum. *Lewis & Clark Law Review*, *19*(1), 115-168.

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75-89.

Zuboff, S. (2020). *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. Public Affairs.