Vol. 33, nº 2

La valorisation des renseignements personnels au Québec et au Canada : la promesse des projets de loi nº 64 et C-11

Pierre-Luc Déziel*

* Professeur agrégé, Faculté de droit, Université Laval.

[Note : cet article a été soumis à une évaluation à double anonymat.]

RÉSUMÉ

Cet article s'intéresse a la propension des projets de loi n° 64 et C-11 à faciliter le traitement de renseignements personnels dans une perspective de valorisation de ces renseignements.

L'article comprend trois parties. Les deux premières s'intéressent à une catégorie de modifications que les projets de loi n° 64 et C-11 mettent en avant afin d'encourager les pratiques de valorisation des renseignements personnels. La première partie porte ainsi sur les mécanismes mis en place pour faciliter l'utilisation et la communication de renseignements personnels à des fins de recherche, d'étude et de production de statistiques, alors que la seconde s'intéresse au renforcement du principe de responsabilité auxquels sont soumis les organismes publics et les entreprises en vertu de la loi.

Dans chacune de ces parties, l'auteur tente à la fois d'expliquer les principales modifications que les projets de loi n° 64 et C-11 apportent aux cadres législatifs actuels et d'identifier les points de convergence et de divergence des approches mises en avant au niveau provincial et au niveau fédéral. Dans la troisième partie, l'auteur cherche à mieux comprendre l'impact que les modifications avancées par les projets de loi pourraient avoir sur les capacités de valorisation des entreprises et des organismes publics en analysant certains enjeux qui pourraient miner leurs efforts de valorisation.

INTRODUCTION

Au cours des derniers mois, les législateurs québécois et canadiens ont déposé d'importants projets de loi visant la modernisation des lois qui encadrent la protection des renseignements personnels au Québec et au Canada. Le *Projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[1], présenté à l'Assemblée nationale du Québec au mois de juin 2020, propose une réforme significative des deux principales lois qui assurent la protection des renseignements personnels au Québec, soit la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « Loi sur l'accès »)[2], qui vise les organismes du secteur public, et la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « Loi sur le privé »)[3], qui vise les entreprises[4]. Le *Projet de loi C-11, Loi de 2020 sur la mise en œuvre de la Charte du numérique*[5], déposé à la Chambre des communes du Canada au mois de novembre 2020, propose quant à lui l'adoption de deux lois. La première, la *Loi sur la protection de la vie privée des consommateurs* (ci-après « LPVPC »), abroge la première partie de la *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « LPRPDE »)[6], qui s'intéresse à la

1. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 1re sess., 42e lég., Québec, 2020 [PL 64].
2. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 [Loi sur l'accès].
3. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 [Loi sur le privé].
4. Notons que le projet de loi nº 64 apporterait également des modifications à 19 autres lois, comme la *Loi concernant le partage de certains renseignements de santé*, RLRQ, c. P-9.0001, ou la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1, qui contiennent des dispositions portant sur la protection des renseignements personnels.
5. *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*, 2e sess., 42e parl., 2020 [PL C-11].
6. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 [LPRPDE].

protection des renseignements personnels dans le secteur privé. La seconde, la *Loi sur le Tribunal de la protection des renseignements personnels et des données*, propose la création d'un tribunal administratif qui entendrait les appels interjetés contre certaines décisions rendues par le Commissaire à la protection de la vie privée du Canada en vertu de la LPVPC.

Les projets de loi nº 64 et C-11 introduisent d'importantes dispositions visant, entre autres, à préciser les exigences relatives à l'obtention du consentement individuel[7], à définir les règles qui doivent guider la collecte et l'utilisation de renseignements personnels à des fins d'identification, de localisation et de profilage[8] et à baliser l'utilisation de renseignements personnels dans le cadre de décisions automatisées[9]. Ils introduisent aussi de nouveaux droits en matière de portabilité des données[10], de déréférencement des contenus en ligne[11] et de recours en dommages-intérêts[12], et viennent renforcer les pouvoirs d'enquête et de sanction des autorités chargées d'assurer le respect de la loi[13]. Bien que ces modifications soulèvent d'intéressantes questions en matière de protection de la vie privée informationnelle, nous avons décidé de nous concentrer ici sur une dimension spécifique des projets de loi nº 64 et C-11, c'est-à-dire leur propension à faciliter la collecte, l'utilisation, la communication et la conservation de renseignements personnels dans une perspective de *valorisation* de ces renseignements.

---

7. PL 64, supra, note 1, art. 9, qui vient ajouter l'art. 53.1 à la Loi sur l'accès, *supra*, note 2, et l'art. 102, qui vient remplacer l'art. 12 de la *Loi sur le privé*, *supra*, note 3. Voir aussi PL C-11, *supra*, note 5, art. 18 et s. de la *Loi sur la protection de la vie privée des consommateurs*.
8. PL 64, *supra*, note 1, art. 18 qui vient ajouter l'art. 65.0.1 à la Loi sur l'accès, *supra*, note 2 et l'art. 99 qui vient ajouter l'art. 8.1 à la *Loi sur le privé*, *supra*, note 3.
9. PL 64, *supra*, note 1, art. 20 qui vient ajouter l'art. 65.2 à la Loi sur l'accès, *supra*, note 2 et l'art. 102 qui vient ajouter l'art. 12.1 à la *Loi sur le privé*, *supra*, note 3. Voir aussi PL C-11, *supra*, note 5, art. 62 et 63 de la *Loi sur la protection de la vie privée des consommateurs*.
10. PL 64, *supra*, note 1, art. 14 qui vient ajouter l'art. 63.5 à la Loi sur l'accès, supra, note 2 et l'art. 95 qui vient ajouter l'art. 3.3 à la *Loi sur le privé*, *supra*, note 3. Voir aussi PL C-11, *supra*, note 5, art. 72 et 120 de la *Loi sur la protection de la vie privée des consommateurs*.
11. PL 64, *supra*, note 1, qui vient ajouter l'art. 28.1 à la *Loi sur le privé*, *supra*, note 3.
12. PL 64, *supra*, note 1, qui vient ajouter l'art. 93.1 à la *Loi sur le privé*, *supra*, note 3. Voir aussi PL C-11, *supra*, note 5, art. 106 de la *Loi sur la protection de la vie privée des consommateurs*.
13. PL 64, *supra*, note 1, art. 150 et 151 qui viennent ajouter les art. 90 et 91 à la *Loi sur le privé*, *supra*, note 3. Voir aussi PL C-11, *supra*, note 5, art 93-95 de la *Loi sur la protection de la vie privée des consommateurs*.

Par valorisation des renseignements personnels, nous entendons l'utilisation de renseignements personnels à des fins secondaires, c'est-à-dire à des fins qui n'étaient pas prévues au moment de la collecte, et pour lesquelles un consentement n'est généralement pas prévu ou obtenu. Cette définition, peut-être un peu technique, mérite sans doute quelques précisions. Le concept de valorisation renvoie à l'idée générale que l'utilisation de renseignements personnels uniquement aux fins qui ont justifié leur collecte ne permettrait pas d'exploiter tout leur potentiel informationnel. Certains jeux de données pourraient faire l'objet d'utilisations secondaires, notamment dans des contextes de recherche, d'innovation ou de développement socio-économique, afin de dégager un savoir et des connaissances qui n'ont pas été révélés par leur traitement initial. La valorisation des renseignements personnels se présente donc comme une forme de recyclage informationnel qui met à l'épreuve certains des principes fondamentaux de traitement de l'information énoncés par les lois canadiennes et québécoises en matière de protection des renseignements personnels.

D'abord, les processus de valorisation des renseignements personnels remettent en question le principe de limitation de l'utilisation, de la communication et de la conservation des renseignements personnels, principe selon lequel les renseignements collectés ne doivent être utilisés et communiqués que pour l'atteinte des objectifs qui ont justifié leur collecte[14], et supprimés lorsque ces fins sont atteintes[15]. Or puisque les processus de collecte de renseignements personnels peuvent être particulièrement longs, complexes et coûteux, le fait de devoir se départir de certains jeux de données déjà traités représente une forme de gaspillage que l'on devrait éviter. Plutôt que de supprimer les renseignements personnels déjà utilisés, il conviendrait de leur donner un second souffle en les utilisant à des fins qui n'étaient pas envisagées au moment de leur collecte.

Ensuite, la volonté d'utiliser les renseignements personnels à des fins secondaires pourrait compromettre la capacité des personnes à consentir à cette nouvelle utilisation de leurs renseignements personnels. En effet, puisque les pratiques de valorisation des données

14. Loi sur l'accès, *supra*, note 2, art. 65.1, *Loi sur le privé*, *supra*, note 3, art. 12 et LPRPDE, *supra*, note 6, principe 4.5 de l'annexe 1.
15. Loi sur l'accès, *supra*, note 2, art. 63.1, 67.2 et 73, *Loi sur le privé*, *supra*, note 3, art. 10 et 12 et LPRPDE, *supra*, note 6, principe 4.5.3 de l'annexe 1. Voir aussi Commission d'accès à l'information du Québec, *La destruction des documents contenant des renseignements personnels*, mars 2014, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_FI_destruction.pdf>.

sont animées par un souci d'efficacité, on jugerait contre-productif d'exiger des organismes publics et des entreprises qui souhaitent valoriser des renseignements personnels de communiquer à nouveau avec les personnes à la source de ces renseignements pour solliciter un second consentement. Il est fréquent que les jeux de données que les entreprises ou les organismes souhaitent valoriser concernent des cohortes de plusieurs dizaines de milliers de personnes. Le temps, l'énergie et les sommes qui sont nécessaires pour contacter ces personnes engagent des investissements qui pourraient s'avérer dissuasifs. C'est dans cette optique que les processus de valorisation sont souvent articulés par le biais d'exceptions au consentement individuel normalement requis pour la collecte, l'utilisation ou la divulgation de renseignements personnels.

Finalement, les pratiques de valorisation des renseignements personnels occasionnent une plus grande circulation des renseignements et exigent, par conséquent, une augmentation des temps de conservation des jeux de données. Si la valorisation des données est animée par un souci d'efficacité, il semble qu'elle soit aussi traversée par une volonté de faciliter l'accès aux données à des fins de recherche et d'innovation dans une perspective de science ouverte et collaborative[16]. Cette approche semble remettre en question la tendance des lois québécoises et canadiennes en matière de protection des renseignements personnels, qui appréhende le droit à la vie privée informationnelle dans une optique personnaliste s'appuyant sur les notions de contrôle individuel et de consentement de la personne. Dans une optique de valorisation des données, les renseignements personnels sont davantage perçus comme une ressource collective dont le traitement permettrait de générer des retombées positives pour l'ensemble de la société. Par exemple, la *Charte canadienne du numérique*, que met en œuvre le projet de loi C-11, avance le principe selon lequel les renseignements personnels des Canadiens et des Canadiennes devraient être « utilisés de façon éthique et à bon escient, pour créer une valeur ajoutée, promouvoir l'ouverture et améliorer la vie des gens, aussi bien au pays qu'ailleurs dans le monde »[17]. Dans

16. Voir, par exemple, Canada, Les sciences et les technologies pour les Canadiens, *Politique des trois organismes sur la gestion des données de recherche*, 15 mars 2021, en ligne : <http://www.science.gc.ca/eic/site/063.nsf/fra/h_97610.html> [Politique 3 Conseils]. Voir aussi Alliance santé Québec, *2021-2024 Planification stratégique*, 23 mars 2021, en ligne : <https://www.alliancesantequebec.com>.
17. Innovation, Sciences et Développement économique Canada, *Charte canadienne du numérique : La confiance dans un monde numérique*, Ottawa, 12 janvier 2021, en ligne : <https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00108.html?open&WT.mc_id=DigitalCharter_GC-partner_banner_fr>.

le même ordre d'idées, certaines propositions de Innovation, Sciences et Développement économique Canada (ci-après « ISDE ») sur la modification de la LPRPDE soulignent l'importance d'encourager l'utilisation des renseignements personnels à des fins de recherche, et envisagent la création de fiducies de données pour assurer la gestion collective des renseignements destinés à des fins de valorisation[18].

Afin d'accroître les capacités de valorisation des organismes publics et des entreprises tout en garantissant la protection des renseignements personnels qui se verront alors davantage mobilisés, les projets de loi nº 64 et C-11 interviennent sur deux plans. Dans un premier temps, ils transforment le cadre législatif actuel de manière à faciliter l'accès aux renseignements personnels qui pourraient être valorisés par les organismes publics et les entreprises. Pour ce faire, des modifications substantielles sont apportées aux mécanismes par lesquels les entreprises et les organismes publics peuvent utiliser et communiquer des renseignements personnels sans le consentement des personnes concernées, lorsque ces renseignements visent des fins de recherche, d'étude ou de production de statistiques. De plus, certaines modifications avancées par les projets de loi nº 64 et C-11 offrent une plus grande flexibilité quant à l'utilisation et à la communication de renseignements dépersonnalisés, et présentent, du moins dans le cas du projet de loi nº 64, l'anonymisation comme une solution alternative à la destruction des renseignements personnels.

Dans un second temps, puisque les processus de valorisation des renseignements personnels impliquent une remise en question de certains des principes qui garantissent la protection de la vie privée des personnes, les projets de loi nº 64 et C-11 mettent en place des dispositifs qui entendent renforcer certaines des obligations imposées aux organismes publics et aux entreprises en vertu de la loi. Ce renforcement ne vise pas une augmentation du contrôle individuel qu'une personne peut exercer sur ses renseignements personnels, mais entend plutôt intervenir directement auprès des entreprises et des organismes publics en musclant la responsabilité qui leur incombe en matière de protection de ces renseignements. Comme nous le verrons, cet effort de responsabilisation se décline sous l'angle de la responsabilité démontrable, et opère une augmentation des niveaux de réflexivité et de réactivité des organismes publics et des

18. Innovation, Sciences et Développement économique Canada, *Renforcer la protection de la vie privée dans l'ère du numérique. Propositions pour moderniser la Loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, 21 mai 2019, en ligne : <https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00107.html>.

entreprises en matière de protection des renseignements personnels qui sont sous leur contrôle.

Cet article comprend trois parties. Les deux premières parties s'intéressent chacune à une catégorie de modifications que les projets de loi nº 64 et C-11 mettent de l'avant afin d'encourager les pratiques de valorisation des renseignements personnels. La première partie porte ainsi sur les mécanismes mis en place pour faciliter l'utilisation et la communication de renseignements personnels à des fins de valorisation, alors que la seconde s'intéresse au renforcement du principe de responsabilité auquel sont soumis les organismes publics et les entreprises en vertu de la loi. Dans chacune de ces parties, nous tenterons à la fois d'expliquer les principales modifications que les projets de loi nº 64 et C-11 apportent aux cadres législatifs actuels et d'identifier les points de convergence et de divergence des approches mises de l'avant au niveau provincial et au niveau fédéral. Dans la troisième partie, nous cherchons à mieux comprendre l'impact que les modifications avancées par les projets de loi pourraient avoir sur les capacités de valorisation des entreprises et des organismes publics en analysant certains enjeux qui, selon nous, pourraient miner leurs efforts de valorisation.

1. L'OUVERTURE À LA VALORISATION : COMMUNICATION ET UTILISATION DES RENSEIGNEMENTS PERSONNELS DANS UNE OPTIQUE DE RECHERCHE

Cette première partie porte sur les modifications apportées par les projets de loi nº 64 et C-11 aux cadres législatifs actuels afin de faciliter l'accès aux renseignements personnels qui peuvent être utilisés dans une perspective de valorisation par les organismes publics et les entreprises. Puisque les projets de loi proposent des modifications qui diffèrent quelque peu en fonction du fait qu'elles visent le secteur public ou le secteur privé, notre démonstration se décline deux temps. D'abord, nous passons en revue les modifications qui visent le secteur public, et tentons de voir comment les projets de loi nº 64 et C-11 entendent encourager l'accès aux renseignements personnels à des fins de valorisation pour les organismes publics. Précisons d'emblée que, puisque certains jeux de données valorisés par des organismes publics peuvent avoir été initialement collectés par des entreprises, certaines dispositions visant la modification de lois s'intéressant au secteur privé sont aussi pertinentes. Ensuite, nous porterons notre attention sur le secteur privé à proprement parler, et

nous nous intéresserons aux mécanismes mis en place par les projets de loi nº 64 et C-11 pour faciliter la valorisation des renseignements personnels par les entreprises, notamment dans une perspective de recherche et de développement internes.

1.1 La valorisation dans le secteur public : transformation des mécanismes d'accès à des fins d'étude, de recherche et de production de statistiques et utilisation à des fins socialement bénéfiques

Dans cette section, nous nous intéressons aux dispositifs que les projets de loi nº 64 et C-11 proposent afin de faciliter la valorisation des renseignements personnels dans le secteur public. Comme nous le verrons, ces dispositifs s'intéressent surtout aux modes d'utilisation et de communication de renseignements personnels à des fins d'étude, de recherche scientifique ou de production de statistiques. De même, comme nous l'avons mentionné en introduction, les modes d'accès aux renseignements personnels s'articulent principalement autour d'exceptions à la règle générale exigeant le consentement des personnes lorsque l'utilisation ou la communication des renseignements personnels visent des fins qui sont secondaires. La sous-section 1.1.1 s'intéresse donc aux modifications apportées aux lois de protection des renseignements personnels s'intéressant au secteur public et la sous-section 1.1.2, aux modifications apportées aux lois visant le secteur privé.

1.1.1 Les modifications apportées aux lois portant sur le secteur public

Puisque le projet de loi C-11 propose l'adoption de la LPVPC, une loi qui ne s'intéresserait qu'au secteur privé, cette sous-section porte uniquement sur les modifications de la Loi sur l'accès proposées par le projet de loi nº 64. Un des principaux défis auxquels sont confrontés les chercheurs québécois est l'accès efficace, dans des délais raisonnables, à de vastes jeux de données comportant des renseignements personnels qui ont été initialement collectés à d'autres fins que des fins de recherche ou dans le cadre d'une autre recherche que celle qu'ils souhaitent entreprendre. L'exercice de valorisation se frappe généralement à la problématique du consentement. En effet, comme discuté plus haut, une des règles générales des lois québécoises en matière de protection des renseignements personnels est que les renseignements personnels doivent être collectés directement auprès de la personne concernée, qui devra être informée des fins pour lesquelles

la collecte est effectuée[19] et, dans le cas du secteur privé, consentir à cette collecte[20]. De manière générale, toutes utilisations de renseignements personnels à d'autres fins que celles initialement prévues doivent à nouveau faire l'objet d'un consentement individuel[21].

L'obtention du consentement individuel de l'ensemble des personnes concernées par les renseignements personnels est un exercice qui peut s'avérer fastidieux, et ce, pour différentes raisons. Les chercheurs prévoient bien souvent de traiter et d'analyser des jeux de données qui concernent des cohortes de plusieurs dizaines de milliers de personnes. Le temps, l'énergie et les fonds qui sont nécessaires pour contacter les personnes visées, leur expliquer le projet de recherche et obtenir leur consentement rendent ces tâches particulièrement longues, voire impossibles. Qui plus est, il peut être particulièrement difficile de retrouver certaines personnes et de les contacter, surtout lorsqu'il est prévu qu'il s'écoule un certain temps entre le moment de la collecte initiale et celui de l'utilisation secondaire. Finalement, et il s'agit peut-être là d'une particularité du milieu de la recherche, l'obligation d'obtenir le consentement individuel des sujets peut introduire des biais et freiner la composition d'un échantillon représentatif, exhaustif ou valide sur le plan scientifique. En effet, certains membres de la population qui, par exemple, craignent ou comprennent mal le milieu de la recherche pourraient avoir tendance à refuser que leurs renseignements personnels soient utilisés à des fins secondaires de recherche, introduisant par le fait même un biais dans la sélection des renseignements qui viendront peupler le jeu de données.

Afin de pallier ces difficultés, les lois de protection des renseignements personnels proposent différentes solutions et permettent, déjà, de faciliter la communication et l'utilisation non consenties de renseignements personnels à des fins de recherche, d'étude ou de production statistiques. Le paragraphe 5 de l'article 59 de la Loi sur l'accès prévoit en effet qu'un organisme public peut communiquer des renseignements personnels, sans le consentement de la personne concernée, à « une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique ». De même, le paragraphe 8 de l'article 18 de la *Loi sur le privé* permet à une entreprise de communiquer des renseignements personnels sans le consentement de la personne visée « à une personne qui est

19. Loi sur l'accès, *supra*, note 2, art. 65 et *Loi sur le privé*, *supra*, note 3, art. 8.
20. *Loi sur le privé*, *supra*, note 3, art. 14.
21. Loi sur l'accès, *supra*, note 2, art. 65.1 et *Loi sur le privé*, *supra*, note 3, art. 12.

autorisée à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique conformément à l'article 21 ou à une personne qui est autorisée conformément à l'article 21.1 ». Dans l'ensemble de ces cas, les personnes qui sont autorisées à utiliser les renseignements personnels à des fins d'étude, de recherche ou de production de statistiques obtiennent cette autorisation auprès de la Commission d'accès à l'information du Québec (ci-après CAI).

L'article 125 de la Loi sur l'accès se lit en effet comme suit :

> La Commission peut, sur demande écrite, accorder à une personne ou à un organisme l'autorisation de recevoir à des fins d'étude, de recherche ou de statistique, communication de renseignements personnels contenus dans un fichier de renseignements personnels, sans le consentement des personnes concernées, si elle est d'avis que :
>
> 1° l'usage projeté n'est pas frivole et que les fins recherchées ne peuvent être atteintes que si les renseignements sont communiqués sous une forme nominative ;
>
> 2° les renseignements personnels seront utilisés d'une manière qui en assure le caractère confidentiel.
>
> […]

Et l'article 21 de la *Loi sur le privé*, comme suit :

> La Commission d'accès à l'information instituée par l'article 103 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1) peut, sur demande écrite, accorder à une personne l'autorisation de recevoir à des fins d'étude, de recherche ou de statistique, communication de renseignements personnels, sans le consentement des personnes concernées, si elle est d'avis que :
>
> 1° l'usage projeté n'est pas frivole et que les fins recherchées ne peuvent être atteintes que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes ;
>
> 2° les renseignements seront utilisés d'une manière qui en assure le caractère confidentiel.
>
> […]

Ainsi, les chercheurs qui souhaitent utiliser des renseignements personnels sans avoir à obtenir le consentement de l'ensemble des personnes visées doivent obtenir l'autorisation d'utiliser ces renseignements auprès de la CAI. Notons, incidemment, que les organismes publics et les entreprises ne se trouvent pas alors dans l'obligation de communiquer ces renseignements aux chercheurs ayant obtenu une telle autorisation. Une des principales critiques formulées à l'égard des mécanismes de communication de renseignements personnels à des fins de recherche par la Loi sur l'accès et la *Loi sur le privé* tient à la multiplication des autorisations qui sont requises et aux délais qu'engendrent ces processus d'autorisation. En effet, les chercheurs qui souhaitent valoriser des renseignements personnels doivent obtenir les autorisations pertinentes auprès des comités d'éthique à la recherche de leurs institutions respectives et obtenir l'accord des organismes publics ou des entreprises impliqués dans l'exercice de partage. De plus, les démarches que doivent effectuer les chercheurs auprès de la CAI sont particulièrement longues et exigent la satisfaction de critères qui, malheureusement, cadrent difficilement avec la réalité de la recherche aujourd'hui[22].

Le projet de loi no 64 entend faciliter le partage et la valorisation des renseignements personnels à des fins d'études, de recherche et de production de statistiques. La Loi sur l'accès et la *Loi sur le privé* sont modifiées de manière à alléger les processus de communication et d'utilisation de renseignements personnels imposées aux chercheurs. Le projet de loi nº 64 supprime en effet le paragraphe 5 de l'article 59 de la Loi sur l'accès, cité plus haut, et modifie l'article 65.1 de la Loi sur l'accès de manière à permettre l'utilisation, par les organismes publics, de renseignements personnels sans le consentement des personnes visées à des fins d'études, de recherche et de statistiques lorsque ces renseignements sont dépersonnalisés[23]. De même, le projet de loi nº 64 introduit les articles 67.2.1, 67.2.2 et 67.2.3 dans la Loi sur l'accès, des articles qui portent sur la communication non consentie, par les organismes publics, de renseignements personnels à des fins d'études, de recherche ou de statistiques. Nous examinons successivement chacun de ces articles.

L'article 67.2.1 précise qu'un « organisme public peut communiquer des renseignements personnels sans le consentement des

22. Voir, par exemple, Pierre-Luc Déziel, « 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 », (2018) 30:3 *Cahiers de propriété intellectuelle* 827.
23. Nous revenons plus loin sur la définition de la dépersonnalisation au sens du projet de loi nº 64 et du projet de loi C-11. Voir *infra*, section 3.2.

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 ». Il prévoit aussi qu'une évaluation des facteurs relatifs à la vie privée (EFVP) doit avoir préalablement permis d'établir, entre autres, qu'il est déraisonnable d'exiger l'obtention du consentement, que la confidentialité des renseignements sera assurée, qu'il n'est possible d'atteindre l'objectif de l'étude qu'avec les renseignements personnels visés et que le critère de nécessité sera respecté[24]. Notons, aussi, que le paragraphe 3 de l'article 67.2.1 prévoit qu'il faille démontrer que l'objectif de l'étude en question « l'emporte », eu égard à l'intérêt public, sur l'impact sur la vie privée que peut engendrer la communication ou l'utilisation de renseignements personnels. À notre avis, cette formulation est quelque peu problématique, puisqu'elle suppose une forme de hiérarchisation des retombées prévues par la recherche et des considérations relatives à la vie privée des personnes. Il nous semblerait préférable de faire allusion à un processus d'équilibration visant à pondérer les retombées anticipées d'une recherche et l'impact sur la vie privée que celle-ci peut engendrer. À cet effet, l'introduction du principe de l'atteinte minimale, indirectement prévu par le critère de nécessité établi au paragraphe 5 de l'article 67.2.1, pourrait contribuer à faciliter cet exercice.

L'article 67.2.2 semble indiquer qu'il reviendra au chercheur d'effectuer l'EFVP prévue à l'article 67.2.1, et précise aussi que celui-ci devra formuler sa demande auprès de l'organisme par écrit, qu'il devra joindre une présentation détaillée de l'activité de recherche et décrire les « différentes technologies qui seront utilisées pour effectuer le traitement des renseignements ». De même, le chercheur devra joindre la décision du comité d'éthique à la recherche de son institution. L'article 67.2.3 s'intéresse, lui, à la conclusion d'une entente de partage des renseignements personnels. Cette entente, qui devra être remise à la CAI et entrera en vigueur 30 jours après sa réception, doit, entre autres, préciser les modalités d'accès aux renseignements personnels par les membres de l'équipe de recherche, interdire toutes formes d'utilisations secondaires, de communication ou d'appariement qui ne sont pas prévus par le protocole de recherche, et établir les conditions relatives à la conservation, à la sécurité et à la destruction des renseignements personnels.

Le résultat net de ce mécanisme est, nous semble-t-il, de retirer l'obligation d'obtenir une autorisation de la CAI et de privilégier le dialogue direct entre les personnes et organismes qui

24. Nous examinons plus en détail les EFVP plus loin. Voir *infra*, section 2.2.

souhaitent collecter des renseignements personnels à des fins d'étude, de recherche ou de production de statistiques et les organismes qui communiqueront ces renseignements, et ce, dans le but d'accélérer le partage de renseignements personnels. À cet effet, l'article 42 du projet de loi nº 64 abroge l'article 125 de la Loi sur l'accès, qui, on l'a vu plus haut, porte sur le pouvoir de la CAI d'octroyer les autorisations de collecte et d'utilisation de renseignements personnels à des fins d'études, de recherche et de statistiques. Nous revenons plus bas sur cette mécanique[25].

1.1.2 Les modifications apportées aux lois portant sur le secteur privé

La sous-section précédente nous a permis d'expliquer certaines des principales modifications apportées par le projet de loi nº 64 à la Loi sur l'accès afin de faciliter les pratiques de valorisation des renseignements personnels des organismes publics au Québec. Nous nous sommes penchés exclusivement sur le projet de loi nº 64 parce que le projet de loi C-11 ne propose pas de modifications de la *Loi sur la protection des renseignements personnels*[26], qui s'applique au secteur public et vise les institutions fédérales. Dans cette sous-section, nous nous intéressons aux modifications apportées aux lois de protection des renseignements personnels dans le secteur privé, mais qui peuvent néanmoins avoir une incidence sur les capacités de valorisation des organismes publics. L'incidence de ces modifications se traduit par une plus grande capacité des entreprises ou organismes publics à communiquer des renseignements personnels à des organismes publics québécois ou à des institutions fédérales, lorsque cette communication vise des fins d'étude, de recherche scientifique ou de production de statistiques. Ainsi, cette sous-section s'intéresse à la fois au projet de loi nº 64 et au projet de loi C-11. Nous commençons par cerner les modifications apportées par le projet de loi nº 64 à la Loi sur le privé. Nous nous tournons ensuite vers certaines dispositions de la LPVPC énoncées dans le projet de loi C-11 qui peuvent nourrir les efforts de valorisation des institutions fédérales.

Les modifications apportées à la *Loi sur le privé* correspondent en large partie à celles apportées à la Loi sur l'accès. L'article 21, qui porte sur les autorisations attribuées par la CAI[27], est modifié de sorte à autoriser la communication de renseignements personnels,

25. Voir *infra*, section 3.1.
26. *Loi sur la protection des renseignements personnels*, L.R.C. (1985), c. P-21.
27. Voir *supra*, sous-section 1.1.1.

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 »[28]. À l'instar de l'article 67.2.1 de la Loi sur l'accès qui est proposé, l'article 21 exige la conduite d'une EFVP. De même, l'article 21.0.1 de la Loi sur le privé, mis en avant par l'article 110 du projet de loi nº 64, précise les modalités de la demande que doit soumettre le chercheur à l'entreprise, alors que l'article 21.0.2 s'intéresse aux détails de l'entente de partage de renseignements qui doit être conclue avec l'entreprise. Les critères et conditions énumérés aux articles 21, 21.0.1 et 21.0.2 de la *Loi sur le privé* sont identiques à ceux trouvés aux articles 67.2.1, 67.2.2 et 67.2.3 de la Loi sur l'accès. De plus, comme c'est le cas pour la Loi sur l'accès, il semble que le résultat net de ce nouveau mécanisme est de permettre le dialogue direct entre les entreprises et les chercheurs en retirant l'obligation pour les chercheurs d'obtenir une autorisation d'utilisation des renseignements personnels auprès de la CAI.

En ce qui a trait à la LPVPC avancée par le projet de loi C-11, nous retiendrons deux dispositions principales. La première est l'article 35, qui porte sur la communication des renseignements personnels d'un individu, sans son consentement et à son insu, lorsque cette communication est réalisée à des fins statistiques, d'étude ou de recherches érudites. La communication visée par l'article 35 n'est permise que si elle est nécessaire pour atteindre ces fins. En d'autres mots, elle ne peut être conduite que si les fins d'étude ou de recherche ne peuvent être accomplies que par le biais de l'utilisation des renseignements personnels visés. L'article 35 précise aussi que la communication ne pourra être effectuée, à l'insu de la personne et sans son consentement, que lorsqu'il sera « pratiquement impossible » d'obtenir son consentement. De même, l'entreprise qui effectue cette communication doit avertir le Commissaire à la protection de la vie privée du Canada avant de communiquer les renseignements.

Deux remarques méritent d'être formulées à l'égard de l'article 35 LPVPC. La première est le fait qu'il remplace l'alinéa 7(3) f) LPRPDE, qui permet déjà le type de *communication* visée par l'article 35 et qui est articulé en fonction des mêmes critères. Toutefois, il est intéressant de noter que la LPRPDE permet aussi, à travers son alinéa 7(2)c), *l'utilisation* de renseignements personnels sans le consentement de l'individu et à son insu, à des fins de statistiques, d'études ou de recherches érudites. L'alinéa 7(2)c) LPRPDE serait remplacé par l'article 21 LPVPC, que nous abordons à la prochaine

28. PL 64, *supra*, note 1, art. 110.

section. Comme nous les verrons, les renseignements personnels ne pourront désormais être utilisés que s'ils ont été dépersonnalisés. La deuxième chose que l'on peut noter à l'égard de l'article 35 est qu'il ne précise pas si une communication doit être effectuée auprès d'une entité du secteur public ou du secteur privé. En ce sens, les deux cas de figure sont envisageables. Néanmoins, il est important de souligner que l'entité privée ou publique qui recevra les renseignements personnels effectuera alors une collecte de renseignements personnels ; cette collecte indirecte devra alors être évaluée en fonction de la loi à laquelle est soumise cette entité.

La seconde disposition de la LPVPC pertinente en matière d'utilisation de renseignements personnels à des fins de valorisation par une entité publique est l'article 39, qui ne trouve pas d'équivalent dans la LPRPDE. L'article 39 permet la communication de renseignements personnels, sans le consentement et à l'insu des personnes visées, lorsque cette communication est faite à une fin qui est « socialement bénéfique ». Cette exception au consentement individuel est intéressante parce que, en reconnaissant la capacité de certaines entités à utiliser ces renseignements dans le but de dégager des retombées qui peuvent être bénéfiques pour la société dans son ensemble, elle établit aussi un lien implicite entre la LPVPC et les pratiques de valorisation des renseignements personnels. L'alinéa 39(1)b) précise en effet que la communication de renseignements personnels peut être faite à une institution gouvernementale au Canada, à des établissements de soins de santé ou d'enseignement postsecondaire situés au Canada, ou à une bibliothèque publique située au Canada. La communication peut aussi être faite à une organisation mandatée, en vertu d'une loi fédérale ou provinciale ou d'un contrat avec une institution fédérale, pour la réalisation d'une fin socialement bénéfique. Cette précision est pertinente puisqu'elle ouvre la porte à la création de banques de renseignements personnels administrées dans une perspective de gestion collective, telle que des fiducies de données[29]. Qui plus est, la définition d'une fin socialement bénéfique comme une fin « relative à la santé, à la fourniture ou à l'amélioration des services et infrastructures publics, à la protection de l'environnement ou de toute autre fin réglementaire »[30] renvoie à

29. Voir, sur ce point, Teresa Scassa, « Data for Good?: An Assessment of the Proposed Exception in Canada's Private Sector Data Protection Law Reform Bill », en ligne (blogue) : <http://www.teresascassa.ca/index.php option=com_k2&view=item&id=335:data-for-good?-an-assessment-of-the-proposed-exception-in-canada's-private-sector-data-protection-law-reform-bill&Itemid=80>.
30. PL C-11, *supra*, note 5, art. 39(2) de la *Loi sur la protection de la vie privée des consommateurs*.

des domaines d'application qui soulèvent des enjeux qui interpellent la société canadienne prise dans son ensemble. Il importe toutefois de remarquer que l'alinéa 39(1)a) LPVPC précise aussi que les renseignements personnels doivent être dépersonnalisés avant que la communication soit effectuée, une thématique que nous abordons à la troisième partie de cet article.

1.2 La valorisation dans le secteur privé : utilisation des renseignements personnels à des fins de recherches internes

La section précédente nous aura permis d'expliquer comment les projets de lois nº 64 et C-11 traduisent une volonté des législateurs québécois et canadiens d'augmenter les capacités de valorisation de renseignements personnels des entités qui évoluent dans le secteur public. Dans cette section, nous portons notre attention sur le secteur privé et tentons de voir comment les modifications prévues à la *Loi sur le privé* et à la LPRPDE viennent transformer les capacités de valorisation des entreprises. À cet effet, nous verrons que les stratégies des législateurs québécois et canadiens sont essentiellement similaires, en ce sens qu'elles permettent toutes deux une plus grande flexibilité en matière d'utilisation, sans le consentement et à l'insu des personnes sources, de renseignements personnels qui sont dépersonnalisés à des fins d'études et de recherches internes.

Le projet de loi nº 64 propose de modifier la *Loi sur le privé* en introduisant la possibilité pour les entreprises d'utiliser des renseignements personnels, sans le consentement de la personne, à des fins d'étude, de recherche ou de production de statistiques[31]. Cette modification est significative, puisque la *Loi sur le privé* ne permet, dans son état actuel, aucune exception à l'obligation pour les entreprises d'obtenir le consentement des personnes concernées pour utiliser leurs renseignements personnels à des fins secondaires. Le nouvel article 12 comporte néanmoins certains éléments qui encadrent l'utilisation secondaire sans le consentement des personnes visées, de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques. Nous en retenons ici quatre principaux. D'abord, les renseignements utilisés doivent être dépersonnalisés. Ensuite, l'utilisation doit être nécessaire pour atteindre les objectifs de l'étude, de la recherche ou de la production de statistiques. Ici, le critère de nécessité renvoie à l'idée que ces objectifs ne peuvent

31. PL 64, *supra*, note 1, art. 102, qui modifie l'art. 12 de la *Loi sur le privé*, *supra*, note 3.

être atteints que si les renseignements personnels sont utilisés[32]. Troisièmement, l'article 12 vise des utilisations qui sont conduites au sein de l'entreprise, donc des activités de recherche ou d'étude qui sont menées à l'interne. L'article 12 ne porte pas, en fait, sur la communication de renseignements personnels, mais bien sur l'utilisation de renseignements personnels par des entités qui exercent déjà un contrôle sur ces renseignements. Finalement, l'article 12 ne précise pas, comme le font par ailleurs les dispositions pertinentes du projet de loi C-11, que l'utilisation secondaire peut être faite à l'insu des personnes concernées. Bien que le projet de loi nº 64 permette des utilisations secondaires sans le consentement des personnes visées, il ne semble pas soustraire de manière explicite les entreprises au devoir d'informer les personnes des fins pour lesquelles leurs renseignements personnels sont utilisés.

Le projet de loi C-11 propose lui aussi certaines modifications qui portent sur la capacité de valorisation des renseignements personnels que détient une entreprise. Notons que, contrairement à la *Loi sur le privé*, la LPRPDE contient déjà une exception au consentement individuel qui permet à une organisation d'utiliser un renseignement personnel à des fins statistiques, d'études ou de recherches érudites. Comme mentionné à la sous-section 1.1.2. de cet article, l'alinéa 7(2)c) LPRPDE permet aux organisations de procéder à de telles utilisations si elles s'avèrent nécessaires à l'atteinte des objectifs de recherche fixés et s'il est « pratiquement impossible » d'obtenir le consentement des personnes visées. Mentionnons aussi que le paragraphe 7(2) LPRPDE précise que l'utilisation de renseignements personnels aux fins visées peut être faite sans le consentement de la personne et à son insu.

L'article 21 LPVPC, qui viendrait en quelque sorte remplacer l'alinéa 7(2)c), apporte toutefois deux précisions supplémentaires. La première est qu'il est clairement établi, à l'instar de l'article 12 de la *Loi sur le privé* tel qu'il est proposé par le projet de loi nº 64, que les fins de recherche et de développement poursuivies doivent être internes, c'est-à-dire qu'elles doivent être menées au sein de l'entreprise. Ensuite, toujours à l'instar de l'article 12 de la *Loi sur le privé*, les renseignements personnels qui sont utilisés doivent être préalablement dépersonnalisés. À cet effet, l'article 20 LPVPC vient

32. Sur le critère de nécessité, voir : Pierre-Luc Déziel, « Est-ce bien nécessaire ? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives », (2019) Barreau du Québec, 465 *Développements récents en droit à a vie privée* 1 [Déziel].

aussi établir qu'une entreprise peut utiliser des renseignements personnels, sans le consentement de la personne ou à son insu, dans le but de les dépersonnaliser. Notons, ici, que nous revenons sur les définitions de la dépersonnalisation proposées par les projets de loi dans la troisième partie de cet article.

Les projets de loi nº 64 et C-11 apportent également certaines modifications aux obligations relatives à la conservation et à la destruction des renseignements personnels une fois que les fins qui justifiaient leur collecte sont atteintes, un enjeu important dans un contexte de valorisation des renseignements personnels. On remarque que les projets de loi adoptent cependant des stratégies qui sont diamétralement opposées. En effet, le projet de loi nº 64 tend vers une augmentation des capacités de conservation des renseignements personnels en présentant l'anonymisation des renseignements comme une solution alternative à leur destruction. À l'inverse, le projet de loi C-11 semble inviter à un resserrement de l'obligation de destruction des renseignements personnels utilisés, en supprimant la possibilité pour les organisations de dépersonnaliser les renseignements au lieu de les détruire.

En ce qui a trait aux modifications apportées par le projet de loi nº 64, il convient de noter d'emblée que la Loi sur l'accès et la *Loi sur le privé* exigent actuellement que les organismes publics et les entreprises détruisent les renseignements personnels une fois que les fins initialement visées par leur collecte ont été atteintes[33]. La modification de l'article 73 de la Loi sur l'accès et la reformulation de l'article 23 de la *Loi sur le privé* offriraient dorénavant le choix aux organismes publics et aux entreprises de détruire *ou* d'anonymiser les renseignements utilisés. Ces modifications sont pertinentes à des fins de valorisation, puisqu'elles offrent la possibilité aux entreprises et aux organismes publics de conserver les renseignements personnels sous une forme anonymisée, plutôt que de les détruire. Ainsi, ces renseignements anonymisés pourront être utilisés à des fins secondaires qui n'étaient pas prévues au moment de leur collecte.

Le projet de loi C-11 adopte, lui, un regard différent sur les pratiques de conservation des renseignements personnels des organisations. En effet, le principe 4.5.3 de la LPRPDE sur la limitation de la conservation exige que les organisations détruisent, effacent ou dépersonnalisent les renseignements personnels lorsque les fins qui ont justifié leur collecte sont atteintes. Bien que la LPRPDE ne

33. Voir *supra*, note 15.

précise pas ce que l'on doit entendre par dépersonnalisation, elle permet néanmoins aux organisations de conserver les renseignements personnels dans un format dépersonnalisé et n'exige pas une destruction complète de ces renseignements une fois que les fins visées sont accomplies. Or, le projet de loi C-11 supprime cette possibilité[34] en exigeant que les organisations procèdent au retrait des renseignements dès lors que les fins qui ont justifié leur collecte sont réalisées. La LPVPC définit par ailleurs le retrait comme la « suppression définitive et irréversible de renseignements personnels »[35]. Or, il est vrai qu'en vertu des articles 20, 21 et 39 LPVPC, étudiés plus haut, les organisations peuvent dépersonnaliser les renseignements personnels qu'elles détiennent et les utiliser, sans le consentement et à l'insu des personnes, à des fins de recherche et de développement internes ou à des fins socialement bénéfiques. Il n'appert toutefois pas de manière évidente, à la lecture du projet de loi C-11, que les organisations pourront dépersonnaliser les renseignements et les conserver indéfiniment dans l'éventualité où ils pourraient contribuer à la réalisation de telles fins.

1.3 Conclusion provisoire

Cette première partie nous a permis de décrire les modifications qu'apporteraient les projets de loi nº 64 et C-11 aux lois de protection des renseignements personnels afin de faciliter l'accès aux renseignements personnels qui peuvent être utilisés par les organismes publics et les entreprises dans une perspective de valorisation. Nous avons vu que plusieurs des modifications proposées, notamment dans le secteur public québécois, entendent accélérer l'accès aux renseignements personnels en décentralisant les processus d'autorisations nécessaires à la communication de renseignements personnels à des fins de recherche, d'étude et de production de statistiques. En ce sens, les modifications apportées à la Loi sur l'accès confieraient aux entités publiques et privées la responsabilité d'établir par elles-mêmes les modalités de cette communication en fonction de critères fixés par la loi. Dans ce but, une des stratégies mises de l'avant par le projet de loi nº 64 serait de contraindre les entités à conduire des EFVP qu'occasionneraient alors le partage et l'utilisation des renseignements personnels. Comme nous l'expliquons dans la prochaine partie, la conduite d'EFVP est aussi au cœur de l'effort de responsabilisation des organismes publics et des entreprises. Précisons aussi

34. PL C-11, *supra*, note 5, art. 53 de la *Loi sur la protection de la vie privée des consommateurs*.
35. *Ibid*., art. 2.

que cette stratégie fait l'objet d'une analyse plus critique dans la troisième partie de cet article.Il nous a aussi été possible d'établir que les projets de loi nº 64 et C-11 offriraient aux entreprises et aux organisations une plus grande flexibilité en matière d'utilisation de renseignements personnels, sans le consentement des personnes concernées, à des fins de développement et de recherches internes. De plus, les projets de loi misent sur la dépersonnalisation pour garantir la protection des renseignements personnels utilisés à ces fins. Nous revenons, dans la troisième partie de cet article, sur les enjeux que soulèvent les définitions de la dépersonnalisation avancées par les projets de loi nº 64 et C-11. Pour le moment, nous souhaitons porter notre attention sur les moyens mis de l'avant par les projets de loi nº 64 et C-11 afin de renforcer le principe de responsabilité auquel sont soumis les entreprises et les organismes publics.

2. LA RESPONSABILITÉ DÉMONTRABLE DES ACTEURS : FAVORISER LA PROTECTION DES RENSEIGNEMENTS PERSONNELS EN ENCOURAGEANT LA RÉFLEXIVITÉ ET LA RÉACTIVITÉ

Dans la mesure où les pratiques de valorisation des données facilitent la circulation des renseignements personnels et réduisent la capacité des personnes à exercer un contrôle effectif sur ceux-ci, il est impératif que les lois mettent en place des dispositifs permettant de veiller à ce que les organismes publics et les entreprises qui en assurent la gestion respectent les obligations qui leur incombent en matière de protection du droit à la vie privée des personnes. Afin de faciliter cet exercice, les projets de loi nº 64 et C-11 viennent muscler les dispositions relatives à la responsabilité des organismes publics et des entreprises en les obligeant à exercer un contrôle plus serré et plus transparent sur leurs pratiques de gestion des renseignements personnels, et en leur demandant d'être en mesure de démontrer qu'ils agissent en conformité avec la loi. Cette responsabilité démontrable, pour reprendre l'expression avancée par certains auteurs[36], exige notamment que les organismes publics et les entreprises mettent en place des programmes de gestion des renseignements personnels qui

36. Voir, par exemple, Ignacio Cafone, « Propositions stratégiques aux fins de la réforme de la LPRPDE élaborées en réponse au rapport sur l'intelligence artificielle », Rapport de recherche remis au Commissariat à la protection de la vie privée du Canada, novembre 2020, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/pol-ai_202011/> [Cafone].

sont sous leur contrôle, mettent sur pied des comités particuliers ou communiquent, sur demande des autorités de réglementation, des documents permettant de démontrer qu'ils agissent en conformité avec la loi. De manière sans doute plus importante, cette responsabilité démontrable exige aussi que les organismes publics et les organisations privées effectuent des EFVP dans la mise en œuvre de certains projets qui impliquent la collecte, l'utilisation et la communication de renseignements personnels. De plus, puisque les pratiques de valorisation des renseignements personnels demandent des temps de conservation plus longs de ces derniers et invitent à une plus grande circulation de ceux-ci, l'encadrement des mesures visant la protection des renseignements personnels semble insister davantage sur l'importance d'assurer une gestion responsable et adéquate des risques d'atteinte à la confidentialité des renseignements personnels.

Dans cette deuxième partie, nous abordons la thématique du renforcement du principe de responsabilité démontrable sous deux angles principaux. Dans un premier temps, nous nous intéressons à l'effort de réflexivité que les projets de loi nº 64 et C-11 invitent les entreprises et les organismes publics à déployer sur les plans de la documentation, de la publication et de l'évaluation des mesures qu'ils adoptent pour assurer une protection adéquate des renseignements personnels qui sont sous leur contrôle (2.1). Dans un deuxième temps, nous portons notre attention sur l'effort de réactivité exgié par les projets de loi nº 64 et C-11 sur le plan de la gestion, de la notification et de la documentation des incidents de confidentialité auxquels peuvent être confrontés les organismes publics et les entreprises (2.2).

2.1 Un effort de réflexivité : documentation, publication et évaluation des mesures adoptées pour protéger les renseignements personnels

Le principe de responsabilité existe déjà dans certaines lois québécoises et canadiennes relatives à la protection des renseignements personnels. Il prévoit que les organismes publics et les entreprises sont responsables des renseignements personnels qu'ils détiennent et qu'ils doivent s'assurer de respecter les obligations que la loi leur impose pour protéger ces renseignements[37]. Les projets de loi nº 64 et C-11 proposent néanmoins un renforcement du principe de responsabilité, renforcement se traduisant, notamment, par l'exigence que les entités publiques et privées fassent preuve d'une plus

37. LPRPDE, *supra*, note 6, principe 4.1 de l'annexe 1.

grande réflexivité relativement aux mesures qu'elles adoptent pour protéger le droit à la vie privée des personnes. Ainsi, la notion de responsabilité se présente non seulement comme la capacité des entités à documenter leurs propres pratiques, c'est-à-dire à les expliciter et à les publier, mais aussi comme la capacité à jeter un regard critique sur celles-ci et à évaluer, sur une base continue, l'impact que certaines de leurs pratiques peuvent avoir sur la vie privée des personnes. Cette réflexivité devrait contribuer à assurer le caractère démontrable de la responsabilité confiée aux organismes publics et aux entreprises.

Le renforcement du principe de responsabilité dans une optique de réflexivité semble particulièrement mis en avant par le projet de loi nº 64. Les modifications proposées à la Loi sur l'accès et à la *Loi sur le privé* visent en effet à obliger les organismes publics et les entreprises non seulement à documenter et à publier les mesures qu'ils prennent pour protéger la vie privée des personnes, mais aussi à conduire des évaluations des facteurs relatifs à la vie privée pour la mise en œuvre de certains projets. Dans le cas des organismes publics québécois, notons que l'article 8 de la Loi sur l'accès précise déjà que la personne responsable de la protection des renseignements personnels est, par défaut, la personne qui détient la plus haute autorité au sein de l'organisme et que ces responsabilités peuvent être déléguées à un membre de l'organisme ou de son conseil d'administration, ou encore à un membre de son personnel de direction[38]. Le projet de loi nº 64 propose toutefois l'ajout de l'article 8.1, qui édicte que les organismes publics québécois devront aussi se doter d'un « comité sur l'accès à l'information et la protection des renseignements personnels » dont le mandat serait de soutenir la personne responsable de la protection des renseignements personnels et d'exercer, comme nous le verrons, diverses fonctions que la loi lui confirait. En ce qui a trait à la *Loi sur le privé*, elle ne précise pas, dans son état actuel, que les entreprises sont responsables des renseignements personnels qu'elles détiennent. Le projet de loi nº 64 remédie à cette situation en créant la section I.1, « responsabilités relatives à la protection des renseignements personnels », qui précise, par le biais de l'article 3.1, qu'une « personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient ». En vertu de cet article, c'est la personne qui possède la plus haute autorité au sein de l'entreprise qui doit veiller à à ce que cette dernière agisse

38. Loi sur l'accès, *supra*, note 2, art. 8. Mentionnons toutefois que le projet de loi nº 64 introduit aussi l'art. 52.2, qui précise de manière plus explicite qu'un organisme public est responsable de la protection des renseignements personnels qu'il détient », PL 64, *supra*, note 1, art. 7.

en conformité avec la loi. La fonction de responsable de la protection des renseignements personnels peut toutefois être déléguée à toute personne.

Le projet de loi nº 64 introduit aussi de nouvelles obligations en matière de documentation et de publication des mesures visant à assurer la protection des renseignements personnels. Nous en retenons ici trois principales. La première s'intéresse à la nécessité, pour les organismes publics et les entreprises, de publier sur leur site Internet des informations détaillées au sujet des règles qui structurent et guident les mécanismes de gouvernance des renseignements personnels qu'ils mettent en place pour veiller au respect de la loi[39]. Ces règles peuvent prendre la forme de politiques, de directives ou de guides qui informent les citoyens et les usagers des rôles et des responsabilités de l'organisation et des membres de son personnel en matière de protection des renseignements personnels[40], mais aussi des processus qui sont mis en place pour le traitement des plaintes. Ces politiques doivent être approuvées soit par le Comité sur l'accès à l'information et la protection des renseignements personnels lorsqu'il s'agit d'un organisme public, soit par le responsable de la protection des renseignements personnels lorsqu'il s'agit d'une entreprise. De plus, le projet de loi nº 64 précise que, dans le cas des organismes publics, les règles publiées doivent décrire les activités de formation et de sensibilisation offertes au membre de son personnel en matière de protection des renseignements personnels[41].

La seconde obligation qui nous semble ici pertinente porte sur la nécessité, pour un organisme public qui collecte des renseignements personnels par le biais d'un moyen technologique, de publier sur son

39. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'article 63.3 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'article 3.2 à la *Loi sur le privé*, *supra*, note 3. Il est peut-être intéressant de souligner que du projet de loi nº 64 précise aussi que les règles mises en place et publiées par les entreprises doivent aussi être « proportionnées à la nature et à l'importance des activités de l'entreprise ».

40. Notons que, dans le cas des entreprises, les politiques et pratiques relatives à la gouvernance des renseignements personnels sont abordées par le projet de loi nº 64 par le biais de la conservation et de la destruction des renseignements personnels. À cet effet, la formulation de l'article 3.2 laisse sous-entendre que l'élaboration et la publication de ces règles sont obligatoires. PL 64, *supra*, note 1, art. 95.

41. Cette précision n'est pas anodine, puisqu'elle porte principalement sur la dimension organisationnelle des efforts de sécurisation des renseignements personnels, c'est-à-dire sur les mesures administratives adoptées par l'organisme pour conscientiser les membres du personnel quant à l'importance de veiller à la protection du caractère confidentiel des renseignements personnels. Nous reviendrons plus bas sur les dispositions portant plus spécifiquement sur la gestion des risques liés à la sécurité des renseignements personnels. Voir *infra*, section 2.2.

site Internet la politique de confidentialité qui régit cette collecte[42]. Cette politique doit être rédigée en des termes simples et clairs, et toute modification à celle-ci doit être communiquée aux personnes visées. Le projet de loi nº 64 et la *Loi sur le privé* ne précisent pas de manière explicite que les entreprises doivent elles aussi publier des politiques de confidentialité. Toutefois, en pratique, la publication de politiques de confidentialité découle directement de l'article 8 de la *Loi sur le privé*, qui porte sur le devoir d'information des fins visées par l'utilisation des renseignements personnels collectés, et sur obligations relatives au consentement prévues à l'article 14 de cette même loi.

La troisième obligation pertinente dans une perspective de réflexivité, et qui est sans doute la plus significative, porte sur la nécessité pour les entreprises et les organismes publics de conduire une EFVP pour « tout projet 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 »[43]. Le comité sur l'accès à l'information et la protection des renseignements personnels de l'organisme public ou le responsable de la protection des renseignements personnels de l'entreprise doit être consulté dès le début du projet[44] et peut, à toute étape de celui-ci, proposer des mesures supplémentaires visant le renforcement de la protection des renseignements personnels[45]. Cette nouvelle obligation est importante dans la mesure où la conduite d'EFVP contraint les organismes publics et les entreprises à réfléchir, dans une perspective critique, à l'incidence que peuvent avoir certaines de leurs activités sur la vie privée des personnes. Puisque les EFVP doivent être accomplies dès le début d'un projet[46], elles encouragent les entreprises et les organismes publics à intégrer la protection de la vie privée dans la conception même d'un projet. Par conséquent, la protection des renseignements personnels n'est pas simplement un

42. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.4 à la Loi sur l'accès, *supra*, note 2.
43. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.5 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'art. 3.2 à la *Loi sur le privé*, *supra*, note 3. Notons aussi que les articles 14 et 95 du projet de loi ont été amendés de manière à préciser que les EFVP doivent être menées uniquement pour les projets d'acquisition, de développement ou de refonte d'un système d»information ou de prestation électroniques de services.
44. *Ibid*.
45. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.6 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'article 3.4 à la *Loi sur le privé*, *supra*, note 3.
46. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.5 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'article 3.2 à la *Loi sur le privé*, *supra*, note 3.

enjeu qui doit être abordé à la suite de la mise en œuvre d'un nouveau programme, mais se présente comme une variable à part entière du processus de design du programme. Ce faisant, la conduite d'EFVP peut être considérée comme un moyen visant à mettre en œuvre la responsabilité des organismes publics et des entreprises[47] et à appuyer le caractère démontrable du niveau de conformité avec la loi[48].

Dans un guide d'accompagnement de mars 2021, la Commission d'accès à l'information du Québec définit l'EFVP comme une « démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques »[49] et qui consiste à « considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées »[50]. Au nombre des facteurs qui doivent être pris en considération, on compte, notamment, le niveau de conformité du projet aux lois applicables en matière de protection des renseignements personnels, l'identification des risques que peut occasionner le projet sur la vie privée des personnes, l'évaluation de l'impact de ces risques sur la vie des personnes, et l'élaboration d'une stratégie pour éviter ou réduire ces risques[51]. On aura donc compris que les EFVP invitent à une prise en charge de la protection des renseignements personnels dans une optique de gestion du risque[52]. À cet effet, il est intéressant de noter que le Commissariat à la protection de la vie privée du Canada définit les EFVP comme « 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 »[53].

Le projet de loi nº 64 ne précise pas quels sont les critères qui doivent être pris en considération lorsqu'une entreprise ou un

47. Voir Cafone, *supra*, note 36.
48. Commissariat à la protection de la vie privée du Canada, *Nos attentes : Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée*, Ottawa, mars 2020, en ligne : <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/#toc4-2> [CPVP].
49. Commission d'accès à l'information du Québec, *Guide d'accompagnement. Réaliser une évaluation des facteurs relatifs à la vie privée*, Québec, 10 mars 2020, en ligne : <https://www.cai.gouv.qc.ca/documents/Guide_EFVP_FR.pdf>.
50. *Ibid*.
51. *Ibid.*, p. 12.
52. Secrétariat du Conseil du Trésor du Canada, *Directive intérimaire sur l'évaluation des facteurs relatifs à la vie privée*, Ottawa, 18 juin 2020, en ligne : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308> [Directive CT].
53. CPVP, *supra*, note 48.

organisme public conduit une EFVP pour l'élaboration d'un projet de système d'information ou de prestation électronique de services qui implique la collecte, l'utilisation ou la divulgation de renseignements personnels. Toutefois, comme le projet de loi contraint également les entreprises et les organismes publics à mener de telles évaluations dans d'autres circonstances, il est possible de déceler quelques éléments qui pourraient s'avérer pertinents. En effet, des EFVP doivent également être produites lorsque les entreprises souhaitent communiquer des renseignements personnels à l'extérieur du Québec[54]. De même, une EFVP doit être effectuée, on l'a vu plus haut, lorsqu'un organisme public ou une entreprise souhaite communiquer des renseignements personnels à une personne ou à un organisme public à des fins d'étude, de recherche ou de production de statistiques sans le consentement de la personne visée[55]. Dans le cas des transferts de renseignements personnels à l'extérieur du Québec, l'entreprise ne pourra effectuer la communication que si une EFVP permet de démontrer que les renseignements personnels transmis jouiront d'une protection qui est jugée adéquate au regard des principes de protection des renseignements personnels généralement reconnus. L'EFVP doit alors notamment tenir compte de la sensibilité du renseignement communiqué, des fins visées par l'utilisation prévue, des mesures visant la protection des renseignements et du régime juridique applicable dans l'État où les renseignements seraient communiqués.

Dans le cas des communications à des fins d'études, de recherche ou de production de statistiques, une EFVP doit être conduite pour étayer cinq conclusions. D'abord, il s'agit de vérifier que la communication de renseignements personnels sous une forme permettant d'identifier la personne est nécessaire à l'atteinte de l'objectif de l'étude, la recherche ou la production de statistiques. Ensuite, comme la communication serait effectuée sans le consentement des personnes sources, il doit être déraisonnable d'exiger des personnes qui conduisent le projet qu'elles obtiennent un tel consentement. Troisièmement, il doit être démontré que l'objectif du projet d'étude, de recherche ou de production de statistiques l'emporte sur l'impact que la communication et l'utilisation des renseignements personnels pourraient avoir sur la vie privée de la personne. Quatrièmement, l'utilisation des renseignements personnels communiqués doit permettre d'assurer leur caractère

54. PL 64, *supra*, note 1, art. 103 qui, vient remplacer l'art. 17 de la *Loi sur le privé*, *supra*, note 3.
55. PL 64, *supra*, note 1, art. 23, qui vient ajouter l'art. 67.2.1 à la Loi sur l'accès, *supra*, note 2 et l'art. 110, qui vient remplacer l'art. 21 de la *Loi sur le privé*, *supra*, note 3.

confidentiel. Finalement, la communication des renseignements personnels doit respecter le principe de limitation, en vertu duquel seuls les renseignements personnels qui sont nécessaires[56] à l'atteinte des fins visées par le projet peuvent être communiqués.

Il convient aussi de souligner que le projet de loi nº 64 ne circonscrit pas l'obligation de conduire des EFVP à certaines situations particulières, c'est-à-dire à des contextes où les projets de système d'information ou de prestation électronique de services pourraient, par exemple, avoir un impact significatif sur la vie privée des personnes. Le projet de loi nº 64 se distingue donc d'autres types d'outils législatifs qui imposent la conduite d'EFVP à certaines entités. Par exemple, le *Règlement général sur la protection des données* européen contraint les responsables du traitement des données à caractère personnel à conduire des analyses d'impact relatives à la protection des données (AIPD) lorsque le traitement visé est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[57]. Ainsi, une AIPD serait notamment requise lorsque le traitement des données vise une évaluation systématique d'aspects personnels des personnes s'appuyant sur un traitement automatisé de l'information et dont le but est de fournir une décision pouvant produire des effets juridiques[58]. En l'absence de tels principes limitatifs, on peut affirmer que le projet de loi nº 64 impose une obligation particulièrement large et particulièrement restrictive pour les entreprises et les organismes publics[59]. Néanmoins, cette obligation invite aussi ces entités à adopter une posture plus réflexive qui les amène à voir la protection de la vie privée des personnes comme un processus continu qui doit traverser les différentes phases d'élaboration d'un projet ou d'un programme impliquant le traitement de renseignements personnels.

Si le projet de loi nº 64 propose d'importantes modifications à la Loi sur l'accès et à la *Loi sur le privé* qui renforceraient le principe de responsabilité, le projet de loi C-11 semble, lui, un peu moins bavard. Il convient toutefois de préciser que le principe de responsabilité est

56. Pour plus d'information sur le principe de nécessité, voir *supra*, note 32.
57. CE, *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*, art. 35.1.
58. *Ibid.*, art. 45, par. 35.3.
59. William Denault-Rouillard et Vanesssa Henri, « Évaluation des facteurs relatifs à la vie privée : la nouvelle réalité pour les organisations québécoises traitant des renseignements personnels ? », 8 septembre 2020, en ligne (blogue) : <https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/09/8-assessments-of-privacy-related-factors/>.

bien établi dans la LPRPDE, puisqu'il figure déjà à l'annexe 1 de la Loi[60]. Dans la LPVPC proposée par le projet de loi C-11, le principe de responsabilité se trouve énoncé aux articles 7 à 11. Ces articles ne modifient pas de manière importante le principe tel qu'on le trouve dans la LPRPDE. En effet, le projet de loi C-11 réitère l'idée qu'une organisation est responsable des renseignements personnels qui sont sous son contrôle[61], et qu'elle doit désigner une ou plusieurs personnes qui auront la responsabilité d'assurer la conformité de ses activités aux exigences de la loi[62]. L'article 9 LPVPC viendrait remplacer le principe 4.1.4 de l'annexe 1 de la LPRPDE. Bien que les deux dispositions soient similaires sur le fond, l'article 9 LPVPC introduit l'obligation pour une organisation de mettre en œuvre un « programme de gestion de la protection des renseignements personnels », une expression que l'on ne trouve pas dans la LPRPDE. Ce programme de gestion doit comprendre, d'une manière toutefois essentiellement similaire aux exigences déjà prévues dans la LPRPDE, les politiques, pratiques et procédures qui sont mises en œuvre pour assurer la conformité avec la loi, et qui sont relatives à la protection des renseignements personnels, à la réception des demandes d'accès, au traitement des plaintes, à la formation du personnel et à l'élaboration de documents qui expliquent les politiques, pratiques et procédures mises en place par l'organisation. Contrairement aux obligations proposées par le projet de loi n° 64, le projet de loi C-11 ne comporte aucune obligation de rendre public le programme de gestion de l'organisation. Toutefois, le projet de loi C-11 propose que la LPVPC permette au Commissaire à la protection de la vie privée du Canada (CPVP) d'avoir, sur demande, accès aux politiques, pratiques et procédures mises en place par l'organisation pour assurer la conformité avec la loi[63].

Contrairement au projet de loi n° 64, le projet de loi C-11 n'envisage pas d'imposer aux organisations la conduite d'EFVP, et semble plutôt mettre en place une stratégie de renforcement du principe de responsabilité démontrable qui se déploie par l'introduction d'un mécanisme d'approbation de codes de conduite et de programmes de certification auquel peuvent se soumettre, sur une base volontaire, les organisations. Le projet de loi C-11 permettrait en effet à une

60. Rappelons que l'annexe 1 de la LPRPDE énumère les dix principes énoncés dans la norme nationale du Canada intitulée *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, auxquels les entreprises doivent se soumettre en vertu du paragraphe 5(1) de la Loi.
61. PL C-11, *supra*, note 5, art. 7(1) de la *Loi sur la protection de la vie privée des consommateurs*.
62. *Ibid.*, art. 8(1).
63. *Ibid.*, art. 10.

organisation ou une institution gouvernementale de demander au CPVP d'approuver des codes de conduite visant la mise en œuvre de pratiques qui assureraient une protection des renseignements personnels équivalente ou supérieure à celle exigée par la loi[64]. De plus, une organisation ou une institution gouvernementale peut demander au CPVP d'approuver des programmes de certification qui comprendraient, entre autres, des codes de pratique, des lignes directrices relatives à l'interprétation de ces codes, un mécanisme permettant à une entité de certifier qu'une organisation est conforme au code de conduite, et des mécanismes de vérification indépendante de la conformité à ce code[65].

La LPVPC octroierait aussi au CPVP certains pouvoirs relatifs à l'approbation et à la gestion des programmes de certification[66]. Non seulement le CPVP pourrait demander à une entité qui gère un tel programme de lui communiquer tout renseignement relatif à ce programme, mais il pourrait aussi révoquer l'approbation donnée à un programme et même recommander à une entité de retirer sa certification à une organisation si celle-ci n'agit pas de manière conforme aux exigences prévues par le programme. Bien que l'adoption d'un code de conduite ou l'adhésion à un programme de certification se fassent sur une base volontaire, et bien que la conformité à un code ou à un programme ne soustraie pas les organisations aux obligations que leur impose la LPVPC, on peut imaginer que ces nouveaux outils permettront aux organisations de jeter un regard critique sur leurs pratiques de protection des renseignements personnels et d'obtenir un avis externe et fiable sur leur niveau de conformité avec la loi. Ainsi, une telle approche permettrait d'inscrire le principe de responsabilité démontrable dans une optique de prévention des atteintes à la vie privée des personnes et d'anticipation des contraventions possibles aux obligations prévues par la loi. Qui plus est, il est possible de supposer qu'un dispositif de vérification externe et indépendant permettrait d'agir de manière complémentaire au travail d'enquête mené par le CPVP[67].

2.2 Un effort de réactivité : la gestion des risques liés à la sécurité des renseignements personnels

La section précédente nous a permis d'examiner les dispositions des projets de loi n^{o} 64 et C-11 qui portent sur le principe

64. *Ibid.*, art. 76.
65. *Ibid.*, art. 77.
66. *Ibid.*, art. 81.
67. Voir Cafone, *supra*, note 36.

de responsabilité démontrable dans une optique de réflexivité des entreprises et organismes publics. Nous avons vu que ces entités seraient invitées à jeter un regard critique sur leurs propres pratiques en matière de protection des renseignements personnels, et ce, afin de s'assurer d'agir en conformité avec la loi. Diverses dispositions portant sur la documentation des pratiques, sur la publication des procédures, sur la mise en œuvre d'activités de formation ou sur l'adoption de codes de conduite viennent articuler ce renforcement du principe de responsabilité des entreprises. À ce sujet, nous avons également constaté que le projet de loi nº 64 insiste sur l'importante significative des EFVP pour assurer une gestion efficace des risques d'atteinte à la vie privée des personnes et de contravention à la loi que peuvent occasionner l'adoption de certains programmes ou de projets nécessitant le traitement de renseignements personnels.

Dans cette section, nous souhaitons nous attarder sur un autre processus qui s'inscrit dans une perspective de gestion des risques, mais qui porte plus spécifiquement sur la capacité des organismes et des entreprises à prévenir, à détecter et à signaler des incidents relatifs à la sécurité des renseignements personnels qui sont sous leur contrôle. Cet accent sur les processus de gestion des incidents relatifs à la sécurité des renseignements est important dans un contexte qui entend promouvoir la valorisation des données. Comme nous l'avons expliqué en introduction, les pratiques de valorisation impliquent une plus grande circulation des renseignements personnels et exigent des temps de conservation plus longs de ces derniers. La mise en réseau des renseignements personnels à des fins de valorisation pourrait en effet les rendre plus vulnérables à certaines actions qui pourraient compromettre leur sécurité. Ainsi, alors que nous avons précédemment évoqué l'effort de réflexivité que devront déployer les organismes et entreprises en vertu des projets de loi nº 64 et C-11, nous souhaitons ici nous intéresser aux efforts de réactivité qu'ils devront aussi mettre en place dans l'éventualité où un incident de sécurité se produirait. Évidemment, les organismes publics et les entreprises doivent être réflexifs sur le plan de la sécurité et travailler de manière à prévenir de tels incidents. Toutefois, ils devront aussi adapter leurs pratiques pour se conformer à certaines des exigences prévues par les lois québécoises et canadiennes en matière de gestion des incidents de sécurité.

Comme ce fut le cas à la sous-section précédente, les principales modifications qui nous intéressent ici sont proposées par le projet de loi nº 64. Ce constat découle sans doute du fait que la LPRPDE comprend déjà plusieurs dispositions importantes en matière de

sécurité des renseignements personnels, et qu'une section particulière sur les atteintes aux mesures de sécurité[68] fut introduite en 2015 par le biais de la *Loi sur la protection des renseignements personnels numériques*[69]. Ainsi, nous nous concentrons ici davantage sur les modifications apportées par le projet de loi nº 64 aux lois québécoises, et utilisons les dispositions existantes de la LPRPDE simplement afin de ponctuer notre analyse.

La Loi sur l'accès et la *Loi sur la privée* imposent toutes deux des obligations relatives à la sécurité des renseignements personnels que détiennent les organismes publics et les entreprises[70]. Les mesures de sécurité déployées par ces entités doivent être proportionnelles à la sensibilité des renseignements, à leur support, à leur quantité et à la finalité de leur utilisation. Toutefois, les lois québécoises en matière de protection des renseignements personnels n'offrent pas beaucoup de précisions quant à la manière dont cette sécurité peut-être assurée, ou sur les obligations et responsabilités la manière dont cette sécurité doit être assurée, ni sur les obligations et responsabilités qui incombent aux organismes publics et aux entreprises dans l'éventualité où surviendrait un incident de confidentialité. Ces lacunes, mises en lumière par l'affaire *Desjardins*[71], sont en large partie corrigées par les modifications proposées par le projet de loi nº 64. En effet, outre les dispositions discutées dans la section précédente, la Loi sur l'accès et la *Loi sur le privé* sont modifiées de manière à définir ce qu'est un incident de confidentialité et à imposer certaines obligations aux entités qui sont confrontées un tel incident.

Ainsi, le projet de loi nº 64 prévoit cinq types d'incidents de sécurité : l'accès non autorisé à un renseignement personnel, l'utilisation non autorisée d'un renseignement personnel, la communication non autorisée d'un renseignement personnel, la perte d'un renseignement personnel ou tout autre atteinte à la protection d'un tel renseignement[72]. Lorsqu'un organisme public ou une entreprise a

68. Il s'agit de la section 1.1 «Atteintes aux mesures de sécurité», qui comprend les articles 10.1 à10.3, LPRPDE, *supra*, note 6.
69. *Loi sur la protection des renseignements personnels numériques*, L.C. 2015, ch. 32.
70. Loi sur l'accès, *supra* note 2, art. 63.1 et *Loi sur le privé*, *supra*, note 3, art. 10.
71. Commission d'accès à l'information du Québec, *Enquête sur la Fédération des caisses Desjardins du Québec*, Dossier 1020846-S, décembre 2020, en ligne : <https://www.cai.gouv.qc.ca/documents/Decision_1020846-11-décembre-2020_VF_diffusion.pdf>.
72. PL 64, *supra*, note 1, art. 14 qui vient ajouter l'art. 63.8 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'article 3.6 à la *Loi sur le privé*, *supra*, note 3. Notons que la définition de l'expression « atteinte aux mesures de sécurité » avancée par l'art. 2 LPVPC est essentiellement similaire : « Communication non

des motifs de croire qu'un incident de confidentialité s'est produit, il doit alors prendre des mesures raisonnables pour limiter les risques qu'un préjudice ne soit causé et éviter qu'un autre incident ne se produise[73]. Puisque des motifs raisonnables sont suffisants, une entité doit réagir même si elle n'est pas convaincue qu'un incident de confidentialité se soit produit. De plus, si l'incident en question présente le risque qu'un préjudice sérieux soit causé aux personnes touchées, les organismes publics et les entreprises doivent à la fois avertir la CAI et les personnes concernées. Ils peuvent aussi, si nécessaire, aviser toute personne ou tout organisme qui peut être en mesure de réduire ce risque[74]. Pour évaluer le risque de préjudice occasionné par un incident de confidentialité, l'entité doit prendre en considération le degré de sensibilité du renseignement, les conséquences que son utilisation peut entraîner et la probabilité qu'il puisse servir à des fins préjudiciables[75]. Si le projet de loi n^{o} 64 n'explique pas ce que peut être une fin préjudiciable, la LPVPC énumère certains exemples, comme la lésion corporelle, l'humiliation, le vol d'identité ou la perte de possibilité d'emploi[76]. Finalement, les organismes publics et les entreprises doivent tenir un registre des incidents dont ils sont victimes et transmettre ce registre, sur demande, à la CAI[77]. Notons, sur ce point, que l'effort de réactivité que le projet de loi n^{o} 64 invite les entreprises et les organismes publics à fournir se décline aussi dans une perspective de documentation et de publication qui est pertinente aux fins du respect du principe de responsabilité démontrable.

2.3 Conclusion provisoire

Cette seconde partie nous aura permis d'établir que la promotion des pratiques de valorisation des renseignements personnels s'accompagne aussi d'un renforcement du principe de responsabilité démontrable. À cet effet, les organismes publics et les entreprises doivent être à la fois plus réflexifs et plus réactifs. L'effort de réflexi-

---

autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues à l'article 57 ou du fait que ces mesures n'ont pas été mises en place », PL C-11, *supra*, note 5.

73. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.7 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'art. 3.5 à la *Loi sur le privé*, *supra*, note 3.
74. *Ibid*.
75. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.9 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'art. 3.7 à la *Loi sur le privé*, *supra*, note 3.
76. PL C-11, *supra*, note 5, art. 58(7) de la *Loi sur la protection de la vie privée des consommateurs*.
77. PL 64, *supra*, note 1, art. 14, qui vient ajouter l'art. 63.8 à la Loi sur l'accès, *supra*, note 2 et l'art. 95, qui vient introduire l'art. 3.8 à la *Loi sur le privé*, *supra*, note 3.

vité s'appuie sur des notions de documentation et de publication des mesures prises pour assurer la protection des renseignements personnels, mais aussi, notamment dans le cadre du projet de loi nº 64, sur l'évaluation des impacts que les pratiques de collecte, d'utilisation et de communication de ces renseignements peuvent occasionner sur la vie privée des personnes. Dans le cadre du projet de loi C-11, nous avons vu que cet effort de réflexivité s'articule aussi en fonction de la possibilité d'avoir recours à des processus de certification et d'approbation de codes de conduite qui encouragent un plus haut degré de conformité avec la loi. Ainsi, l'effort de réflexivité que doivent manifester les organisations est complété par des processus d'accompagnement que mettent en place des organismes indépendants et externes sous la supervision du CPVP. En ce qui a trait à l'effort de réactivité prévu par les projets de loi nº 64 et C-11, il se présente principalement sous la forme qui doivent être adoptées par les organismes publics et les entreprises lorsqu'il est raisonnable de croire qu'un incident de confidentialité s'est produit. Ces mesures visent une gestion prudente et transparente du risque que l'incident de confidentialité occasionne un préjudice aux personnes concernées.

3. DISCUSSION : CERTAINES DIFFICULTÉS SOULEVÉES PAR LES PROJETS DE LOI Nº 64 ET C-11 EN MATIÈRE DE VALORISATION DES RENSEIGNEMENTS PERSONNELS

Les deux premières parties de cet article nous ont permis de montrer que la promotion des pratiques de valorisation des renseignements personnels envisagées par les projets de loi nº 64 et C-11 s'articule en deux temps ; d'abord, en facilitant l'utilisation et la communication de renseignements personnels à des fins de recherche, d'étude et de production de statistiques, et ensuite, en renforçant les obligations relatives au respect du principe de responsabilité démontrable que les lois imposent aux entités qui utilisent ou communiquent ces renseignements personnels. À cet effet, l'augmentation des capacités de valorisation des entreprises et des organismes publics se traduit par la mise en place de mécanismes visant, entre autres, une décentralisation des processus d'autorisation pour accéder à des renseignements personnels, une plus grande flexibilité en matière d'utilisation de renseignements dépersonnalisés, une ouverture à la conservation de renseignements anonymisés et une obligation d'agir de manière plus réflexive et réactive en matière de gestion des risques liés au traitement de renseignements personnels.

Dans cette section, nous souhaitons expliquer pourquoi certaines de ces mesures pourraient produire des effets indésirables tant sur le plan de l'augmentation des capacités de valorisation des organismes publics et des entreprises que sur le plan de l'affermissement souhaité de la protection de la vie privée des personnes concernées. Nous abordons deux enjeux principaux. Dans un premier temps, nous revenons sur les dispositions visant la décentralisation des mécanismes d'autorisation de communication et d'utilisation de renseignements personnels à des fins de recherche, d'étude et de production de statistiques dans le secteur public (3.1). Plus précisément, nous montrons que cette décentralisation pourrait s'avérer contre-productive dans la mesure où elle pourrait fort bien imposer des délais supplémentaires aux organismes publics, aux entreprises et aux chercheurs qui souhaitent utiliser des renseignements personnels ou les communiquer dans une perspective de valorisation. Selon nous, afin d'accélérer les mécanismes d'autorisation tout en assurant un haut niveau de protection de la vie privée des personnes concernées, il conviendrait d'orienter les processus.... non pas vers les projets de recherches individuels, mais bien vers les équipes de chercheurs les processus d'évaluation qui sous-tendent les mécanismes d'autorisation non pas sur les projets de recherches individuels, mais bien sur les équipes de chercheurs et les centres de recherche. Cette possibilité est surtout intéressante si elle est articulée en fonction d'un renforcement du principe de responsabilité démontrable déjà prévu par les projets de loi.

Dans un second temps, nous nous concentrerons sur les définitions de renseignements personnels dépersonnalisés et de renseignements personnels anonymisés proposées par les projets de loi nº 64 et C-11 (3.2.). Nous nous intéresserons plus particulièrement aux différences qu'affichent ces définitions et à l'impact qu'elles peuvent avoir sur la capacité des entreprises et des institutions publiques à utiliser des renseignements dépersonnalisés ou anonymisés tout en garantissant un degré élevé de protection de la vie privée des personnes. Selon nous, les définitions offertes par le projet de loi nº 64 sont inadéquates et peuvent compromettre les pratiques de valorisation qu'il entend mettre en avant. Plus précisément, la définition de renseignement dépersonnalisé est trop vague et soulève des enjeux en matière de protection de la vie privée et la définition de renseignement anonymisé est trop restrictive et engendre des problèmes d'ordre plus pratique.

3.1 La décentralisation des mécanismes d'autorisation de communication et d'utilisation de renseignements personnels à des fins de recherche

Comme discuté dans la première partie de cet article, un des principaux objectifs du législateur avec l'adoption du projet de loi nº 64 semble être celui de faciliter l'utilisation et la communication de renseignements personnels à des fins d'étude, de recherche et de production de statistiques. Pour ce faire, la Loi sur l'accès et la *Loi sur le privé* seraient modifiées de manière à évacuer la nécessité, pour les chercheurs, d'obtenir une autorisation préalable auprès de la CAI pour le traitement de renseignements personnels à de telles fins. Dans la mesure où l'obtention de ces autorisations représente de considérables investissements de temps, et où les différentes autorisations que doivent obtenir les chercheurs sont multipliées, il est raisonnable de penser qu'un mécanisme visant le dialogue direct entre les chercheurs, les organismes publics et les entreprises allégerait les processus d'échange des renseignements personnels et encouragerait la valorisation de ces derniers dans un contexte d'innovation et de progrès scientifique. Néanmoins, ces nouvelles façons de faire ne sont pas sans soulever de nouvelles inquiétudes. Nous en retiendrons ici trois principales.

Dans un premier temps, le fait de retirer la CAI des processus de demande de partage des renseignements personnels pousse les organismes, les entreprises et les chercheurs à interpréter eux-mêmes les critères et les conditions énoncés dans la loi en matière d'utilisation et de communication de renseignements personnels à des fins de recherche. Une des principales craintes tient au fait que la multiplication des interprétations de ces critères par les différents acteurs impliqués pourrait aussi entraîner un problème d'uniformisation de l'application de la loi et, par conséquent, diminuer la prévisibilité de celle-ci. Si les chercheurs sont aujourd'hui généralement rompus aux réalités des processus de demandes auprès de la CAI et savent comment adapter leurs demandes en fonction de son interprétation des critères énoncés dans les lois, ils pourraient se retrouver demain confrontés à des interprétations qui différeront en fonction de l'organisme ou de l'entreprise qu'ils approchent, complexifiant par le fait même le processus de demande.

Dans un second temps, le processus d'autorisation de la CAI actuellement en place doit aussi être perçu comme permettant une forme de contrôle par un tiers neutre, indépendant et compétent. Cette autorisation confère une forme d'objectivité et de légitimité au

processus et apporte ainsi une certaine assurance à l'organisme ou à l'entreprise invitée à partager les renseignements personnels que les critères énoncés dans la loi sont bel et bien respectés. Dans une certaine mesure, l'obtention de l'autorisation de la CAI sert de mesure incitative au partage des données. À l'inverse, il est à craindre que les évaluations effectuées par les chercheurs eux-mêmes quant à l'importance de leurs recherches et de l'impact de celles-ci sur la vie privée puissent être perçues, à tort ou à raison, comme plus subjectives et intéressées.

Dans un troisième temps, l'obligation pour le chercheur de conduire une EFVP pour chaque demande d'accès aux renseignements personnels alourdit de manière importante les processus de collecte de renseignements, mais exige aussi des connaissances, compétences et expertises qui peuvent largement dépasser le domaine de spécialisation des chercheurs[78]. La conduite d'une EFVP rigoureuse est un exercice complexe qui exige un travail minutieux et technique[79]. L'obligation de conduire une EFVP viendrait aussi ajouter à d'autres tâches similaires et connexes que les chercheurs doivent déjà accomplir lorsqu'ils déposent des demandes auprès de leurs comités d'éthique à la recherche (ci-après CÉR). De plus, au mois de mars 2021, les principaux organismes subventionnaires fédéraux – les Instituts de recherche en santé du Canada, le Conseil de recherches en sciences humaines et le Conseil de recherches en sciences naturelles et en génie – ont adopté une politique exigeant que les chercheurs élaborent et décrivent, dans leurs demandes de subvention, des plans de gestion des données de recherche[80]. La superposition d'une obligation de conduire une EFVP aux exigences relatives à l'élaboration de plans de gestion des données – qui incluent les renseignements personnels – et aux procédures mises en place par les CÉR pourrait entraîner la multiplication même des barrières à l'accès aux données que le projet de loi n° 64 semble vouloir éviter.

En somme, il semblerait que, plutôt que de résoudre le problème de l'accès aux données dans une perspective de valorisation

78. Notons que, dans le cadre des consultations particulières et auditions publiques sur le projet de loi n° 64, plusieurs intervenants ont aussi souligné le fardeau important qu'impose aux entreprises la conduite d'EFVP. Voir, Québec, Commissions des institutions, *Rapport sur les consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels. Procès-verbaux des séances des 22, 23, 24 et 29 septembre 2020*, Dépôt à l'Assemblée nationale n° 1858-20200930, 2020, en ligne : <http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci/mandats/Mandat-43315/index.html>.
79. Voir, par exemple, Directive CT, *supra*, note 52.
80. Voir Politique 3 Conseils, *supra*, note 16.

des renseignements personnels à des fins de recherche, le projet de loi nº 64 déplace ce problème. Bien que l'obligation actuelle d'obtention d'une autorisation d'utilisation de renseignements personnels sans le consentement des personnes concernées amène certaines lourdeurs qui peuvent ralentir le processus d'accès aux données, le problème n'est pas en soi le rôle qu'est invitée à jouer la CAI, mais porte plutôt sur deux facteurs particuliers.

D'abord, la CAI accomplit un travail exhaustif et conduit une analyse particulièrement rigoureuse des demandes qui lui sont soumises. C'est d'ailleurs cette minutie qui qui nourrit la confiance des chercheurs, des organismes publics, des entreprises, mais aussi des citoyens en matière de protection des renseignements personnels qui sont communiqués à des fins de recherche. Toutefois, ces examens sont longs et demandent d'importantes ressources. À notre avis, un des principaux problèmes auquel est confrontée la CAI est le manque de ressources qui sont mises à sa disposition. Ainsi, une partie du problème pourrait être résolu en octroyant davantage de ressources à la CAI, des ressources qui devraient être exclusivement dédiées au traitement des demandes d'autorisation de communication et d'utilisation de renseignements personnels à des fins d'étude, de recherche et de production de statistiques. Ces ressources pourraient aussi permettre à la CAI de jouer un rôle d'accompagnement auprès des chercheurs dans la mise en place de pratiques et politiques assurant la protection de la vie privée. Ensuite, le milieu scientifique reproche souvent à la CAI un certain « biais » à l'endroit de la protection de la vie privée et souligne son incapacité à prendre en compte les réalités de la recherche scientifique contemporaine. Selon nous, ces difficultés résultent en grande partie de la nature du mandat qui est confié à la CAI – soit celui de veiller à la protection des renseignements personnels – et surtout, du cadre juridique et réglementaire au sein duquel elle doit opérer. En effet, plusieurs des critères qui sont prévus dans les lois de protection des renseignements personnels et certains des principes qui les sous-tendent comme le critère de nécessité[81], limitent grandement le partage de renseignements personnels parce qu'ils s'agencent mal avec la manière dont les projets de recherche sont aujourd'hui développés.

Un élément de solution aux différents enjeux soulevés dans cette section serait, à notre avis, la reconnaissance du milieu de la recherche comme un secteur distinct d'activité qui, bien qu'entretenant certaines similitudes avec le secteur privé et le secteur public,

81. Voir Déziel, *supra*, note 32.

soulève des enjeux particuliers en matière de protection de la vie privée et de traitement des renseignements personnels. En d'autres termes, les chercheurs ne mènent pas des projets qui adoptent des logiques relevant de l'administration publique ou de la conduite d'activités commerciales. De même, ils ne sont pas animés par le même type d'objectifs ou d'intérêts. Par exemple, l'identité des personnes concernées est rarement pertinente ; le chercheur n'entend généralement pas contacter la personne dans le cadre d'une prestation de service, d'un paiement ou d'une offre publicitaire. Dans le même ordre d'idée, les programmations scientifiques et les méthodes de recherche et de traitement des données des chercheurs ont souvent fait l'objet d'un examen par les organismes subventionnaires, par les pairs et par les comités d'éthique à la recherche de leurs institutions.

Bien qu'il soit nécessaire d'encadrer, nécessaire d'encadrer sérieusement, les activités de recherche qui exigent l'utilisation ou la divulgation de renseignements personnels, l'encadrement actuel et l'encadrement proposé par le projet de loi n° 64 opèrent peut-être à un niveau qui n'est pas adéquat. Le modèle actuel et le modèle envisagé visent en effet un encadrement des *projets* de recherche et des opérations de traitement des renseignements personnels qu'ils proposent, alors qu'ils devraient s'intéresser à l'encadrement des *chercheurs* – ou des Centres de recherche – eux-mêmes. Les lois de protection des renseignements personnels devraient abandonner cette approche de l'encadrement « à la pièce » pour adopter une approche plus systémique. Une telle approche allégerait les processus d'accès aux données, donnerait plus de flexibilité aux chercheurs, accélérerait le partage des données et garantirait un haut degré de protection de la vie privée des citoyens. De même, le renforcement du principe de responsabilité auquel devraient être soumis les chercheurs par le biais de pratiques réflexives et réactives viendrait sans doute assurer une meilleure conformité avec la loi. Toutefois, pour les raisons exposées plus haut, cette responsabilisation des chercheurs ne devrait pas se faire au moyen d'obligations portant sur la conduite d'EFVP, mais devrait s'articuler autour de processus de certification et d'audit qui, s'inspirant du projet de loi C-11, assureraient un niveau adéquat de conformité avec la loi.

De tels modèles existent d'ailleurs déjà au Canada et au Québec. Ces modèles opèrent sur la base de processus de gestion collaborative des données, de systèmes d'autorisation des accès individuels en fonction en fonction des compétence et de l'expertise des chercheurs ou intervenants, de processus d'audit, et de mécanismes robustes permettant d'assurer la confidentialité et la traçabilité des données. En

Ontario, par exemple, l'Institute for Clinical Evaluative Sciences (ICES) agit comme une banque de données et de renseignements personnels sur la santé mise à la disposition de chercheurs pour la conduite de recherches et d'études dans le domaine de la santé. L'ICES agit comme une « entité prescrite » au sens de l'article 45 de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*[82] de l'Ontario, ce qui lui permet de collecter et d'utiliser les renseignements personnels sur la santé de divers dépositaires de ce type de renseignements, comme les cliniques, les hôpitaux, les laboratoires ou les maisons de soins de longue durée[83]. Les chercheurs de l'ICES – ils sont plus de 200 – sont nommés aux termes d'un processus de candidature et de vérification rigoureux et peuvent, une fois l'accréditation obtenue, travailler avec l'ensemble des données disponibles. Les chercheurs font l'objet d'audits réguliers pour conserver leurs droits d'accès aux données. Ainsi, ce ne sont pas les *projets* qui sont approuvés à la pièce, mais bien les *chercheurs* eux-mêmes[84]. Une telle mécanique permet une plus grande flexibilité en termes de recherche, notamment en ce qui a trait à l'appariement des jeux de données, et permet de court-circuiter certains délais superflus. De plus, un important mécanisme de reddition de compte est mis en place, permettant au Commissariat à l'information et à la protection de la vie privée de l'Ontario de réviser, sur une base régulière, les pratiques et politiques de l'organisme en matière de protection de la vie privée[85].

Au Québec, la *Loi concernant le partage de certains renseignements de santé* (ci-après « LCPCRS ») propose un modèle qui s'apparente à celui développé par l'ICES[86]. L'objectif de la LCPCRS est de faciliter la circulation des renseignements personnels sur la santé en assurant « la mise en place d'actifs informationnels permettant le partage de renseignements de santé jugés essentiels aux services de première ligne et au continuum de soins, afin d'améliorer la qualité et la sécurité des services de santé et des services sociaux ainsi que

82. *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, c. 3, ann. A [Loi de 2004].
83. Voir le portail de l'Institute for Clinical Evaluative Sciences, sous l'onglet « Working with ICES data », en ligne : <https://www.ices.on.ca/Data-and-Privacy/ICES-data/Working-with-ICES-Data>.
84. Voir le portail de l'Institute for Clinical Evaluative Sciences, sous l'onglet « Become an ICES Scientist » en ligne : <https://www.ices.on.ca/Research/Information-for-researchers/ICES-Scientist-Appointment-Application-Instructions>.
85. Voir le portail de l'Institute for Clinical Evaluative Sciences, sous l'onglet « Working with ICES data » en ligne : <https://www.ices.on.ca/Data-and-Privacy/ICES-data/Working-with-ICES-Data>.
86. *Loi concernant le partage de certains renseignements de santé*, RLRQ, c. P-9.0001 [LCPCRS].

l'accès à ces services »[87]. Pour ce faire, la LCPCRS établit six banques de données s'intéressant à différents domaines cliniques : les médicaments, les résultats de laboratoire, l'imagerie médicale, l'immunisation, les allergies et les sommaires d'hospitalisation[88]. La LCPCRS met également en place un système de gestion des autorisations d'accès[89] qui permet d'attribuer à certains intervenants[90] ou organismes[91] du milieu de la santé la possibilité de consulter les banques de données. De plus, l'article 106, qui n'est par ailleurs pas encore en vigueur, permet à la CAI de fournir l'autorisation à une personne d'utiliser les renseignements contenus dans les banques de données à des fins de recherche, d'étude ou de statistiques en fonction des critères établis par l'article 125 de la Loi sur l'accès. Évidemment, l'article 91 du projet de loi nº 64 modifie l'article 106 LCPCRS en substituant à l'article 125 de la Loi sur l'accès l'article 67.2.1 discuté plus haut[92]. Notons toutefois que, dans ce cas, l'accès attribué au chercheur vise un projet en particulier. Il importe aussi de préciser que les renseignements personnels qui sont emmagasinés dans les actifs informationnels prévus par la LCPCRS sont confidentiels[93] et que la CAI dispose de certains pouvoirs pour veiller au respect de la vie privée des personnes concernées par les renseignements[94]. Par ailleurs, le paragraphe 1 de l'article 2 LCPCRS précise que la loi doit être interprétée de manière à assurer le respect du droit à la vie privée de la personne et du secret professionnel. Ces deux exemples tendent à démontrer qu'il est possible d'envisager un modèle d'encadrement de la recherche qui favorise le partage et la diffusion des renseignements personnels tout en assurant un haut degré de protection de la vie privée, non pas en exerçant un contrôle granulaire et « à la pièce » sur les projets de recherche, mais plutôt grâce à une gestion des accès aux données attribués à des intervenants autorisés, compétents et imputables.

3.2 Les définitions problématiques du renseignement dépersonnalisé et du renseignement anonymisés

Comme discuté plus haut, les projets de loi no 64 et C-11 facilitent les pratiques de valorisation des renseignements personnels des entreprises et des organismes publics dans une optique de recherche

87. *Ibid.*, art. 1.
88. *Ibid.*, art. 11.
89. *Ibid.*, art. 56.
90. *Ibid.*, art. 69.
91. *Ibid.*, art. 71.
92. Voir *supra*, sous-section 1.1.1.
93. LCPCRS, *supra*, note 86, art. 99.
94. *Ibid.*, art. 132 à 134.

et de développements internes, et misent sur la dépersonnalisation pour garantir la protection des renseignements personnels utilisés. Toutefois, les projets de loi s'en remettent aussi des définitions différentes de ce qu'est un renseignement personnel *dépersonnalisé*. La principale différence entre ces deux définitions tient à la détermination, ou non, d'un seuil acceptable en ce qui a trait au risque de réidentification des personnes sources que l'utilisation de renseignements dépersonnalisés occasionne. Afin de saisir cette différence, quelques précisions sur l'état actuel du droit nous semblent pertinentes. De manière générale, la dépersonnalisation renvoie à un processus par lequel les identifiants directs ou indirects liés à un renseignement personnel sont supprimés, généra-lisés ou modifiés dans le but de camoufler l'identité de la personne qui en est la source. Bien que la dépersonnalisation soit une mesure efficace de protection de la vie privée des personnes concer-nées, plusieurs études déjà bien connues démontrent que le risque de réidentifier les personnes sources, notamment par le biais de techniques de croisement de données, demeure toujours présent.[95]. Ainsi, plusieurs du renseignement personnel qui existent déjà en droit canadien vont tracer la ligne de démarcation entre un renseignement personnel et un renseignement dépersonnalisé en fonction du risque de réidentification que le traitement d'un renseignement peut occasionner.

Par exemple, dans l'arrêt *Gordon* c. *Canada (Santé)*, la Cour fédérale du Canada définit un renseignement personnel comme un renseignement « concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources. »[96]. De même, la *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario définit les renseignements identificatoires comme des renseignements qui permettent « d'identifier un particulier ou à l'égard desquels il est raisonnable de prévoir, dans les circons-tances, qu'ils pourraient servir, seuls ou avec d'autres, à en identifier un ».[97]. Le *Health Information Act* de la Saskatchewan définit, elle, un renseignement dépersonnalisé comme « personal health information that cannot reasonably be expected, either by itself or when combined with other information

95. Voir, par exemple, Jonathan Mayer, Patrick Mutchler et John C. Mitchell, « Evaluating the privacy properties of telephone metadata », (2016) 113:20 *Proceedings of the National Academy of Sciences* 5536, ou Y.-A. De Montjoye, L. Radaelli, V. K. Singh et A. S. Pentland, « Unique in the shopping mall: On the reidentifiability of credit card metadata », (2015) 357: 6221 *Science* 536.
96. *Gordon* c. *Canada (Santé)*, 2008 CF 258, par. 34.
97. *Loi de 2004*, *supra*, note 82, art. 4(2).

available to the person who receives it, to enable the subject individuals to be identified »[98]. Ces quelques exemples montrent que les définitions de ce qu'est un renseignement personnel et, *a fortiori*, un renseignement personnel dépersonnalisé sont articulées autour de critères qui prennent en considération le risque d'identification ou de réidentification que présente le croisement de données. La définition de *Gordon* c. *Canada (Santé)* pose le seuil des « fortes probabilités » d'identification, alors que la loi de l'Ontario s'appuie sur le critère du « raisonnable de prévoir dans les circonstances » et la loi de la Saskatchewan sur celui du «reasonably be expected ».

À l'instar des définitions proposées par la jurisprudence fédérale et par certaines lois provin-ciales, le projet de loi C-11 définit le verbe dépersonnaliser au moyen d'un critère qui permette de fixer clairement le seuil de dépersonnalisation et d'assurer une meilleure prise en charge du risque de réidentification. Ainsi, la dépersonnalisation est présentée comme le fait de :

> « [m]odifier des renseignements personnels — ou créer des renseignements à partir de renseignements personnels — au moyen de procédés techniques afin que ces rensei-gnements ne permettent pas d'identifier un individu ni ne puissent, dans des circons-tances raisonnablement prévisibles, être utilisés, seuls ou en combinaison avec d'autres renseignements, pour identifier un individu ».[99]

Toutefois, le projet de loi no 64 n'établit pas de tel seuil, puisqu'il considère qu'un renseigne-ment personnel sera dépersonnalisé « lorsque ce renseignement ne permet plus d'identifier directe-ment la personne concernée »[100]. Cette définition est, selon nous, problématique puisqu'elle est trop large et ne permet pas une prise en charge adéquate des risques de réidentification que présente l'utilisation de renseignements per-sonnels dans une perspective de valorisation.

En effet, un jeu de renseignements personnels qui ne révèle pas directement l'identité des per-sonnes pourrait être qualifié de dépersonnalisé au sens du projet de loi nº 64, et ce, même s'il était possible de prévoir que son utilisation permettrait la réidentification

---

98. *The Health Information Protection Act*, SS 1999, c. H-0.021, art. 3(2)(a).
99. PL C-11, *supra*, note 5, art. 2 de la *Loi sur la protection de la vie privée des consommateurs*.
100. PL 64, *supra*, note 1, art. 19, qui vient remplacer l'art. 65.1 de la Loi sur l'accès, *supra*, note 2 et l'art. 102, qui vient remplacer l'art. 12 de la *Loi sur le privé*, *supra*, note 3.

indirecte des personnes à la source des renseignements. Bien que cette définition offrirait aux organismes publics et aux entre-prises une grande latitude en matière de valorisation des renseignements personnels, elle est peut-être trop généreuse, en ce sens qu'elle ne protège que timidement la vie privée des personnes.

Il importe toutefois de mentionner que ce risque serait toutefois balisé par différents facteurs. D'abord, en vertu du projet de loi no 64, les organismes publics et les entreprises ne pourraient utiliser des renseignements personnels dépersonnalisés sans le consentement des personnes visées qu'à des fins de développement et de recherche internes. Ensuite, à l'instar de la *LPRPC*[101],le projet de loi nº 64 interdit clairement toute forme de tentative de réidentification à partir de ren-seignements qui ont été dépersonnalisés[102].

Finalement, les amendements récents au projet de loi no 64 qui touchent l'article 65.1 de la Loi sur l'accès et à l'article 12 de la *Loi sur le privé* précisent que les entreprises et les organismes publics doivent « prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés ». En adoptant ces amendements, le législateur québécois reconnait le risque inhérent de réidentification que l'utilisation de renseignements dépersonnalisés représente pour la vie privée et impose certaines obligations aux organismes publics et aux entreprises pour limiter ce risque. Néanmoins, il est aussi important de souligner que ces amendements ne viennent pas modifier la définition de ce qu'est un renseignement dépersonnalisé au sens de la loi. Ils ne portent que sur les mesures qui doivent être prises pour limiter le risque de réidentification, mais ne qualifient pas le niveau de risque qui est acceptable et que les organismes ou les entreprises doivent s'assurer d'atteindre. Si les mesures visant à limiter le risque de réidentification doivent être raisonnables, le niveau de risque à atteindre demeure, lui, relativement flou. Bien que les amendements apportés au projet de loi nº 64 apportent certaines précieuses précisions relativement aux moyens qui doivent être déployés pour assurer une meilleure gestion du risque de réidentification, ils restent vagues sur la portée des fins à atteindre. Ainsi, nous croyons qu'il serait pertinent pour le législateur québécois de mieux circonscrire la définition de la dépersonnalisation que le projet nº 64 en établissant clairement le niveau de risque de réidentification qu'il considère comme acceptable.

---

101. PL C-11, *supra*, note 5, art. 75 de la *Loi sur la protection de la vie privée des consommateurs*.
102. *Ibid.*, art. 74.

En ce qui a trait à la définition de l'anonymisation proposée par le projet de loi nº 64, la problé-matique se voit renversée. Rappelons, sur ce point, que le projet de loi nº 64 présente l'anonymisation comme une solution à la destruction des renseignements personnels une fois que les fins qui ont justifié leur collecte sont atteintes. La définition de l'anonymisation pourrait s'avérer toutefois ici trop stricte, puisqu'elle permet de qualifier un renseignement d'anonymisé « lorsqu'il est raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne »[103]. On remarque que la définition de l'anonymisation porte sur l'impossibilité d'identifier à nouveau les personnes à la source des renseignements ; l'anonymisation doit tendre vers l'*irréversibilité*. Cette condition pourrait s'avérer particulièrement contraignante, voire même irréaliste, pour les en-treprises et les organismes publics qui souhaitent conserver des renseignements personnels pour à des fins de valorisation. En effet, plusieurs études tendent à démontrer que des renseignements en apparence banals et rigoureusement dépersonnalisés peuvent néanmoins être analysés de manière à révéler l'identité des personnes, notamment lorsqu'ils sont croisés avec d'autres jeux de données[104]. Il pourrait ainsi s'avérer problématique pour les entreprises et les organismes publics de clamer l'irréversibilité de l'anonymisation, notamment dans un contexte où il est difficile d'anticiper ce que les innovations technologiques permettront ou non de faire à l'avenir. Dans une telle situation, il est envisageable que les organismes publics et les entreprises adoptent une posture plus prudente, et préfèrent détruire les renseignements personnels plutôt que de les conserver sous un format qui pourrait éventuellement se révéler contraire aux exigences de la loi. Ainsi, les efforts déployés par le législateur pour faciliter la conservation de renseignements personnels pourraient être sapés par les réalités techniques des entreprises et des organismes publics.

Ici aussi, les difficultés que soulèvent la définition de l'anonymisation sont allégées par certains amendements apportés projet de loi nº 64. Notons d'abord l'introduction du seuil « raisonnable de prévoir dans les circonstances » qui ne se trouvait pas dans la définition initiale. Cette modification est importante puisqu'elle permet de qualifier un renseignement d'anonymisé sans avoir à garantir une irréversibilité absolue du processus d'anonymisation. Ensuite, les amendements au projet de loi nº 64 précisent que les organismes

103. PL 64, *supra*, note 1, art. 28 qui vient remplacer l'art. 73 de la Loi sur l'accès, *supra*, note 2 et l'art. 111, qui vient remplacer l'art. 23 de la *Loi sur le privé*, *supra*, note 3.

104. Voir *supra*, note 95.

publics et les entreprises devront anonymiser les renseignements personnels « selon les critères et modalités déterminés par règlement. » Cette modification est im-portante puisqu'il permettra au gouvernement d'adopter des règlements précisant les pratiques d'anonymisation qui doivent être adoptées, dictant par le fait même aux entreprises et organismes publics la voie à suivre pour agir de manière conforme aux exigences de la loi.

CONCLUSION

Les projets de loi nº 64 et C-11 traduisent une volonté d'accroître les capacités de valorisation des renseignements personnels des organismes publics et des entreprises. Ils entendent mettre en place des mécanismes dont l'objectif serait de faciliter la communication et l'utilisation de renseignements personnels à des fins de recherche scientifique, d'innovation technologique et de développement social. De plus, ces projets visent un renforcement de différents aspects de la protection offerte par la loi qui pourraient se révéler plus vulnérables dans un contexte de valorisation des données. Ces objectifs sont, selon nous, importants et méritoires. Néanmoins, nous avons identifié trois volets du projet de loi nº 64 qui, en l'état actuel, pourraient compromettre l'atteinte de ces objectifs. Les premiers portent sur les enjeux que soulève la décentralisation des mécanismes d'autorisation de communication et d'utilisation de renseignements personnels à des fins de recherche sur les plans de la prévisibilité du droit, de la légitimité des autorisations et des délais occasionnés par la conduite d'EFVP. À cet effet, nous soutenons que la loi devrait abandonner l'approche visant à évaluer les projets de recherche de manière individuelle et opter pour une approche plus systémique qui s'intéresserait à la responsabilité de l'équipe ou des centres de recherche. Le second volet porte sur la définition de la dépersonnalisation qui, à notre avis, est trop large et protège mal la vie privée des personnes. Sur ce point, nous pensons que la définition du renseignement dépersonnalisé devrait fixer un seuil clair au-delà duquel les risques de réidentification sont trop importants pour qu'un renseignement puisse être qualifié de dépersonnalisé. Finalement, nous considérons que la définition de l'anonymisation est trop stricte pour être opératoire en pratique. À cet effet, la définition de l'anonymisation ne présente pas une réelle solution alternative à la destruction des renseignements personnels, soit une solution qui serait souhaitable dans une perspective de valorisation des renseignements personnels.