Ministère de la Justice Canada
Department of Justice Canada

MODERNISATION DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS* : DOCUMENT DE DISCUSSION

1. Principes de protection des renseignements personnels et modernisation des règles à l'ère numérique

Un engagement technique auprès d'experts quant à l'avenir de la *Loi sur la protection des renseignements personnels*, la loi fédérale en matière de protection des renseignements personnels s'appliquant au secteur public.

Nous partageons ce document de discussion avec des intervenants experts pour obtenir leurs points de vue et leurs commentaires sur les considérations techniques et juridiques à prendre en compte dans le cadre de la modernisation de la *Loi sur la protection des renseignements personnels*. Cet engagement technique ciblé aidera le Gouvernement du Canada à peaufiner les propositions de modifications à la *Loi sur la protection des renseignements personnels.*

Canada

Table des matières

Renouvellement des relations avec les citoyens à l'ère numérique

La transformation du monde numérique change fondamentalement les attentes, les espoirs et les craintes de la population canadienne par rapport aux façons dont leurs renseignements personnels peuvent être utilisés par toutes sortes d'acteurs publics et privés. Cette transformation élargit considérablement le domaine du possible, remodelant ce qui nous permet de nous épanouir comme citoyens et comme êtres humains. Elle modifie également notre façon d'envisager nos rapports aux personnes et à la société, de communiquer et d'obtenir des services, et ce qui permet au gouvernement de fournir un soutien à la population, de la protéger et d'assurer une réglementation adéquate. À l'ère numérique, la circulation des renseignements personnels est rapide, complexe et omniprésente. Ces renseignements ont maintenant le potentiel contradictoire de nous rapprocher des autres citoyens ou de nous en dissocier, de nous aider ou de nous nuire personnellement, et d'accroître ou de miner notre confiance dans les institutions fédérales. L'évolution du contexte a d'importantes conséquences sur les relations des citoyens entre eux et avec les institutions fédérales, relations qui sont au cœur de la *Loi sur la protection des renseignements personnels*.
La *Loi sur la protection des renseignements personnels* constitue le cadre juridique qui régit le traitement des renseignements personnels dans le secteur public fédéral. Elle explique comment ces renseignements doivent être protégés dans le contexte des relations entre les individus et les institutions fédérales.

La *Loi* énonce les objectifs légitimes pour lesquels les institutions fédérales peuvent recueillir, utiliser et communiquer des renseignements personnels, tant au regard des personnes concernées que dans l'intérêt public en général. Elle établit en outre une structure juridique qui prévoit des restrictions et des conditions quant à la façon dont ces institutions peuvent utiliser et communiquer des renseignements personnels.

Les institutions fédérales doivent s'adapter à l'évolution des attentes des Canadiennes et des Canadiens par rapport à l'usage de leurs renseignements personnels, et elles doivent répondre à leurs préoccupations. Par exemple, les membres de la population canadienne s'attendent de plus en plus à obtenir facilement un accès intégré aux services gouvernementaux, au moyen des plateformes et des appareils qu'ils utilisent déjà. C'est pourquoi le gouvernement du Canada s'emploie à améliorer son offre de services, notamment en rendant leur prestation plus intégrée de façon à optimiser l'expérience des personnes qui les reçoivent. Cela dit, les gens n'ont pas tous le même degré de tolérance quant à la façon dont leurs renseignements personnels pourraient circuler au sein des institutions fédérales et de l'une à l'autre, et quant aux circonstances pouvant le justifier[1].
La révision de la *Loi sur la protection des renseignements personnels* en fonction de la transformation du monde numérique, des exigences d'aujourd'hui et des objectifs gouvernementaux représentera un élément essentiel pour répondre aux attentes de la population canadienne.

La modernisation de la *Loi* vise à faire en sorte que l'échange de renseignements entre les personnes et les institutions fédérales soit régi par des pratiques raisonnables, respectueuses et responsables, qui tiennent compte des défis actuels que la société doit relever en la matière. Cette modernisation donne l'occasion d'y intégrer un rigoureux cadre éthique pour guider la gestion consciencieuse et responsable des renseignements personnels dans le secteur public d'une manière qui est respectueuse des droits des individus par rapport à leurs renseignements personnels. Une fois modifiée et soutenue par de solides mécanismes de transparence, de supervision et de transparence, la *Loi* devrait aider les Canadiennes et les Canadiens à faire confiance à leur gouvernement en ce qui concerne la protection de leurs droits et la gestion de leurs renseignements personnels en cette ère numérique.

Le présent document de discussion technique invite les experts à se pencher sur la question de l'introduction de nouveaux principes de protection des renseignements personnels, accompagnée de règles modernisées, pour guider les interactions des institutions fédérales avec les individus. La question plus générale consiste à

[1] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2019/por_2019_ca/#toc2-6

savoir si – et, le cas échéant, comment – il faudrait intégrer de nouveaux principes de protection des renseignements personnels à la *Loi* afin d'assurer la protection des droits des individus à la vie privée. Renouveler les relations avec les citoyens à l'aide d'un cadre juridique qui tient compte de leurs attentes contemporaines, constitue l'ultime objectif.

A. Nouveaux principes de protection des renseignements personnels pour soutenir une éthique de gestion rigoureuse et responsable favorisant le respect des exigences

Le rythme des changements technologiques et sociaux et les interrelations entre les deux font constamment évoluer nos préoccupations à l'égard des renseignements personnels. Les personnes sont de plus en plus portées à interagir avec les institutions fédérales à l'aide de réseaux numériques, et à utiliser ces réseaux pour leur envoyer des demandes. Pour aider les institutions fédérales à relever les défis variables de la transformation numérique, il serait utile d'introduire des principes visant à intégrer les normes appropriées dans notre cadre fédéral de protection des renseignements personnels. De plus, un cadre fondé sur des principes permet d'établir les résultats attendus, lesquels peuvent servir de base pour inspirer confiance dans la façon dont les institutions fédérales traiteront les renseignements personnels.

Bon nombre de régimes juridiques de protection des renseignements personnels sont inspirés des principes énoncés en 1980 par l'Organisation de coopération et de développement économiques (OCDE), dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel* (qui ont été mises à jour en 2013). En matière de protection des renseignements personnels, tant dans le secteur public que dans le secteur privé, une pratique exemplaire de plus en plus reconnue consiste à s'appuyer sur une approche fondée sur des principes, en l'accompagnant au besoin de lignes directrices plus détaillées[2]. Au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) reflète ce genre d'approche, et ailleurs dans le monde, c'est notamment le cas du *Règlement général sur la protection des données* (RGPD) de l'Union européenne et de la loi australienne sur la protection des renseignements personnels (*Privacy Act*), récemment mise à jour.

Plusieurs témoins entendus au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (comité ETHI) au cours de sa plus récente étude de la *Loi sur la protection des renseignements personnels* ont souligné l'importance d'inclure dans la *Loi* des principes de protection des renseignements personnels qui respectent la neutralité technologique; certains ont souligné l'importance de rédiger la loi de façon relativement générale, en veillant à ce qu'elle soit fondée sur des principes et ne privilégie aucune technologie en particulier. D'autres témoins ont proposé de mettre à jour la disposition énonçant l'objet de la *Loi*, de façon à y mentionner expressément ses objectifs sous-jacents. De fait, le comité ETHI a recommandé que l'objet de la *Loi* soit modifié pour inclure des principes de protection des renseignements personnels qui soient neutres au plan technologique, généralement acceptés et comparables à ceux figurant dans la LPRPDE.

Il y a plusieurs rôles que les principes de protection des renseignements personnels pourraient jouer dans la version modernisée de la *Loi sur la protection des renseignements personnels*. Ils pourraient :

- Expliquer un certain nombre d'engagements fondamentaux que les institutions fédérales peuvent prendre envers les individus concernant leurs renseignements personnels, et qui pour le moment ne font pas partie des exigences législatives expressément énoncées dans la *Loi*;

[2] Voir par exemple les chapitres 4 et 18 du rapport 108 de la commission australienne de réforme du droit (en anglais) : Law Reform Commission, Report 108, *Australian Privacy Law and Practice* <https://www.alrc.gov.au/publications/report-108>.

- Assurer l'harmonisation de la protection des renseignements personnels entre les secteurs public et privé en imposant aux institutions fédérales le même genre de réglementation que celle reconnue et soutenue par le secteur privé;
- Aider le Canada à assurer l'interopérabilité avec l'Europe, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et d'autres États influencés par les lignes directrices révisées de l'OCDE et ceux qui sont susceptibles d'emboîter le pas ultérieurement;
- Guider la prise de décisions discrétionnaires impliquant des renseignements personnels;
- Donner aux institutions fédérales des occasions accrues d'innover pour trouver les meilleurs moyens de protéger les renseignements personnels tout en améliorant l'efficacité dans l'atteinte des autres objectifs;
- Permettre des traitements de renseignements personnels qui ne sont pas expressément autorisés par les dispositions législatives lorsqu'ils sont fondés sur l'intérêt public.

Certains principes pourraient servir à énoncer les normes ou les objectifs qui sous-tendent un certain nombre de règles actuelles. D'autres pourraient instituer des concepts entièrement nouveaux dans le régime législatif. D'autres encore pourraient imposer des obligations concrètes de résultats, alors que certains pourraient plutôt servir à guider l'exercice de pouvoirs discrétionnaires. Quant à déterminer exactement quels nouveaux principes pourraient être intégrés à la *Loi* et comment on pourrait le faire, cela dépend de bon nombre de considérations, et notamment de la façon dont les règles déjà établies seraient ultimement modernisées.

En quoi de nouveaux principes de protection des renseignements personnels pourraient-ils améliorer la Loi sur la protection des renseignements personnels?

Énoncer les engagements fondamentaux pour répondre aux attentes	Encourager les décisions responsables dans les situations inédites	Favoriser l'innovation dans la façon d'atteindre les résultats
Veiller à ce que les pratiques des institutions fédérales relatives aux renseignements personnels répondent aux attentes des individus et reflètent les valeurs canadiennes essentielles à une gouvernance efficace.	*Permettre à la Loi de guider efficacement les institutions fédérales dans un contexte de changements rapides, continus et profonds*	*Faciliter les approches individualisées et innovatrices ainsi que leur amélioration continue, selon un cadre fondé sur des principes*

(i) Répondre aux attentes des individus

L'AJOUT DE NOUVEAUX PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS AIDERAIT LES INSTITUTIONS FÉDÉRALES À RÉPONDRE AUX ATTENTES DES INDIVIDUS ET À REFLÉTER LES VALEURS CANADIENNES ESSENTIELLES À UNE GOUVERNANCE EFFICACE

La *Loi sur la protection des renseignements personnels* s'applique aux renseignements personnels que les individus confient aux institutions fédérales. Elle établit un certain nombre de règles qui déterminent *dans quels cas* les institutions fédérales peuvent recueillir, utiliser et communiquer des renseignements personnels, et comment ces renseignements doivent être traités une fois recueillis. Cette approche fondée sur des règles décrit *dans quels cas* certaines pratiques sont permises, mais elle n'explique pas *pourquoi* ces règles sont importantes ou quelles considérations devraient guider leur application. De plus, la disposition énonçant l'objet de la *Loi* est principalement descriptive – elle n'énonce pas expressément les valeurs fondamentales sur

lesquelles la *Loi* s'appuie. Il s'ensuit que la *Loi sur la protection des renseignements personnels* ne précise pas vraiment les valeurs ou les résultats attendus qui devraient guider la prise de décisions en la matière.

Il pourrait s'avérer utile de prévoir expressément un cadre supplémentaire fondé sur des principes, particulièrement s'il attire l'attention sur ce qui importe le plus aux individus : les pratiques relatives aux renseignements personnels sont-elles raisonnables, proportionnées, justes et éthiquement fondées, sont-elles conformes à l'intérêt public, et protègent-elles adéquatement la vie privée? Pour appuyer ces objectifs, les nouveaux principes de protection des renseignements personnels pourraient énoncer les nouvelles responsabilités et les nouveaux engagements des institutions fédérales à l'égard des Canadiennes et des Canadiens.

(ii) Adaptation au changement continu et perturbateur :

L'AJOUT DE NOUVEAUX PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS PERMETTRAIT À LA* LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS *DE GUIDER EFFICACEMENT LES INSTITUTIONS FÉDÉRALES DANS UN CONTEXTE DE CHANGEMENTS RAPIDES, CONTINUS ET PROFONDS.

Le recours à des règles fixes et prescriptives – qui disent plus ou moins précisément ce qu'il faut faire dans une situation donnée – ne peut vraiment être efficace que si tous les éléments de l'enjeu réglementaire à résoudre sont connus et demeurent relativement inchangés au fil du temps. Or, dans le domaine de la protection des renseignements personnels, les pressions à venir demeurent manifestement incertaines; les changements rapides et perturbateurs constituent la seule constante; et les solutions réglementaires prennent forcément du retard par rapport aux nouvelles technologies.

Les principes constituent généralement des énoncés généraux qui précisent des valeurs abstraites ou des résultats souhaités. Ils laissent le champ libre pour adapter les résultats à toutes sortes de situations, selon ce qui convient aux circonstances. Lorsque les principes établissent des normes de référence capables de résister à l'épreuve du temps, c'est leur généralité et leur souplesse qui constituent leur force réglementaire. Ainsi, quand de nouveaux scénarios se présentent, les institutions sont obligées de se demander comment obtenir les résultats requis, ce qui leur permet de développer leurs capacités institutionnelles et de réagir de manière réfléchie, peu importe la situation à résoudre.

Par exemple, les membres de la population canadienne s'attendent de plus en plus à obtenir facilement un accès intégré aux services gouvernementaux, au moyen des plateformes et des appareils qu'ils utilisent déjà. À cet égard, le gouvernement du Canada est déterminé à améliorer la prestation de services en procurant aux utilisateurs une expérience où ils n'ont pas à fournir leurs renseignements plus d'une fois. Le gouvernement cherche aussi à intégrer harmonieusement son offre de services dans la vie des Canadiennes et des Canadiens, notamment par l'intégration de ces services à des plateformes préétablies. La modernisation de la Loi sur la protection des renseignements personnels *peut servir à intégrer les normes fondamentales appropriées pour permettre la transformation numérique du gouvernement, d'une façon qui favorisera la protection des renseignements personnels détenus par les institutions fédérales, tout en facilitant la prestation de services utilisant le numérique et en favorisant l'obtention de résultats.*

De même, le gouvernement a élaboré récemment la Charte canadienne du numérique, *qui énonce des principes formant « un cadre pour assurer le leadership continu du Canada dans l'économie fondée sur le numérique et les données. Ces principes aideront non seulement à protéger les données et les*

renseignements personnels des Canadiens, mais également à tirer parti des talents et des forces uniques du Canada pour profiter pleinement de la transformation dans le domaine du numérique et des données »[3].

(iii) Soutien de l'innovation selon un paradigme de respect et de responsabilisation :

L'INTÉGRATION DE PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA LOI PEUT FACILITER LES APPROCHES INDIVIDUALISÉES ET INNOVATRICES AINSI QUE LEUR AMÉLIORATION CONTINUE À L'INTÉRIEUR DU CADRE JURIDIQUE ÉTABLI

Le fait de s'en remettre uniquement à des règles précises et détaillées peut dissuader les institutions fédérales d'en faire plus que ce que ces règles exigent expressément. Par exemple, une règle exigeant que l'information soit publiée d'une façon particulière risque de décourager l'usage de façons nouvelles et améliorées de communiquer cette information. Les principes peuvent quant à eux permettre ou encourager l'adaptabilité, aussi bien en matière de protection des renseignements personnels que sur le plan des pratiques opérationnelles, pourvu que cela respecte le cadre juridique applicable. L'adoption de principes de protection des renseignements personnels adéquats peut aider l'innovation et la protection des renseignements personnels à se soutenir mutuellement et à progresser ensemble.

Quelles sont les principales difficultés liées à l'intégration de nouveaux principes de protection des renseignements personnels?

Le recours à de nouveaux principes de protection des renseignements personnels ne suffira pas à moderniser la *Loi*. En fait, bon nombre des avantages de passer à un régime fondé sur des principes peuvent aussi occasionner certaines difficultés. Si on se contente de souligner le résultat à atteindre pour répondre aux attentes, plutôt que de préciser les moyens que l'institution doit prendre pour y parvenir, on risque de se retrouver avec des incohérences entre les différentes approches adoptées. De plus, une réglementation fondée uniquement sur des principes peut compliquer la supervision et le respect de la mise en application des exigences, puisque les limites peuvent alors s'estomper entre, d'une part, les responsabilités dont il faut rendre compte et, d'autre part, les rôles généraux que doivent jouer les institutions pour déterminer les exigences particulières à respecter. Il faut donc trouver un juste équilibre entre l'intégration de nouveaux principes et la modernisation des règles. Il importe également de réfléchir soigneusement aux ajustements qu'il faudrait apporter aux mécanismes de supervision.

Quels principes pourraient être ajoutés à la Loi sur la protection des renseignements personnels?

1. *Raisonnabilité et proportionnalité*

LES PRATIQUES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DOIVENT ÊTRE RAISONNABLES ET PROPORTIONNÉES, CE QUI PASSE NOTAMMENT PAR LE FAIT DE LIMITER LE PLUS POSSIBLE TANT LES CONSÉQUENCES NÉGATIVES POUR LES INDIVIDUS QUE LE RISQUE QU'ELLES SURVIENNENT, ET PAR L'ÉTABLISSEMENT D'UN JUSTE ÉQUILIBRE ENTRE LES INTÉRÊTS CONCERNÉS.

Lorsqu'il s'agit de protection des renseignements personnels, le contexte est important. À cet égard, il pourrait être utile de compter sur un principe directeur de raisonnabilité et de proportionnalité qui s'appliquerait à toutes les pratiques relatives aux renseignements personnels, y compris la collecte, l'utilisation, la communication et

[3] Voir https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2019/05/le-ministre-bains-presente-la-charte-canadienne-du-numerique.html

la conservation. Pour atteindre les mêmes buts que les principes connexes utilisés ailleurs, ce principe de raisonnabilité et de proportionnalité pourrait s'appuyer sur les normes juridiques canadiennes qui sont bien établies en la matière. Par exemple, selon le principe de « minimisation des données » (ou minimalisation des données) qui est énoncé dans le *Règlement général sur la protection des données* (RGPD) de l'UE, les entités visées sont tenues de veiller à ce que les données à caractère personnel soient « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Le fait d'introduire un principe de raisonnabilité et de proportionnalité dans la *Loi sur la protection des renseignements personnels* permettrait de soumettre les pratiques des institutions fédérales à des normes reconnues et essentiellement équivalentes en matière de protection des renseignements personnels – normes juridiques qui sont solidement ancrées dans le droit administratif et le droit relatif à la *Charte canadienne des droits et libertés*.

Certains témoins entendus par le comité ETHI ont précisément recommandé l'adoption d'une obligation générale de proportionnalité qui s'appliquerait à toute collecte, conservation, utilisation ou communication de renseignements personnels par les institutions fédérales. D'autres ont proposé de soumettre la collecte et les usages secondaires de renseignements personnels à un principe de proportionnalité.

Un principe de « raisonnabilité et proportionnalité » amènerait les institutions à évaluer et à atténuer les répercussions et les risques relatifs aux renseignements personnels, même dans les cas où l'action concernée (p. ex. la communication) serait expressément autorisée. Ce principe obligerait les institutions à mettre en œuvre des pratiques de protection des renseignements personnels raisonnables et proportionnées, notamment en ce qui concerne le pouvoir de divulguer des renseignements personnels dans l'intérêt public. Pour que les pratiques en question soient jugées raisonnables et proportionnées, il faudrait que leurs répercussions sur la vie privée soient atténuées. Cependant, aucun moyen particulier ne serait imposé et on n'exigerait pas forcément que l'atteinte soit strictement minimale. Selon le principe de raisonnabilité et de proportionnalité, les institutions fédérales auraient à prendre leurs décisions en se fondant sur une approche globale et équilibrée d'atténuation des répercussions et des risques, et en tenant toujours compte du contexte.

Q.1(a) : Le fait d'imposer un principe de raisonnabilité et de proportionnalité permettrait-il d'atteindre le même but (minimisation raisonnable des données) qu'une norme fondée sur la « nécessité », mais d'une façon qui serait plus aisément adaptable au contexte? Voir aussi la partie du présent document intitulée « Seuil justifiant la collecte », pour de plus amples renseignements et une analyse connexe.

Q.1(b) : Un principe de raisonnabilité et de proportionnalité offrait-il du soutien aux institutions fédérales cherchant à promouvoir l'utilisation des « Données numériques pour le bien commun », en utilisant l'information de façon éthique et dans l'intérêt public?

Q.1(c) : Le principe de raisonnabilité et proportionnalité constitue-t-il un moyen utile et efficace d'intégrer à la Loi sur la protection des renseignements personnels un encadrement juridique qui reflète l'approche du droit canadien en matière des droits de la personne canadien, qui préconise un équilibre entre les droits fondamentaux des individués avec des intérêts public importants (p. ex. l'article 1 de la Charte canadienne des droits et libertés), et reflète les obligations sous-jacentes du droit administratif (p. ex. l'exercice raisonnable d'un pouvoir discrétionnaire)?

2. *Protection des renseignements personnels dès la conception*

TOUTE INSTITUTION FÉDÉRALE DOIT TENIR COMPTE DE L'IMPÉRATIF DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DÈS LA CONCEPTION LORSQU'ELLE CRÉE OU MODIFIE SES PROGRAMMES, SES SERVICES, SES SYSTÈMES OU SES PRATIQUES DE FONCTIONNEMENT.

La protection des renseignements personnels dès la conception constitue désormais une bonne pratique largement reconnue, puisque les décisions prises au moment de la conception peuvent avoir ensuite des

effets importants sur la vie privée. Cette approche est généralement plus efficace et moins coûteuse que celle qui consiste à tenter de régler les problèmes en la matière après le fait. Le rapport de 2018 au greffier du Conseil privé, intitulé *Feuille de route de la Stratégie de données pour la fonction publique fédérale*, souligne que, lorsque les données utilisées ont des implications relatives à la vie privée, les ministères et organismes devraient tenir compte de l'impératif de protection de ces données dès l'étape de la conception.

Une approche de protection des renseignements personnels dès la conception contribuerait à l'intégration des valeurs de protection des renseignements personnels dans la conception des systèmes, empêchant ainsi qu'elles deviennent une source de friction après la mise en œuvre des systèmes en question. Le principe de « protection des renseignements personnels dès la conception » pourrait aussi favoriser l'élaboration de systèmes gouvernementaux améliorés et plus dignes de confiance, ce qui améliorerait l'expérience des intervenants. Par exemple, cela pourrait susciter la confiance nécessaire pour améliorer la prestation de services au moyen d'approches plus innovatrices, en assurant la prise de mesures appropriées pour protéger les renseignements personnels dès la conception des programmes.

Q.1(d) : Le fait d'introduire une obligation de « protection des renseignements personnels dès la conception » permettrait-il de protéger effacement la vie privée? Si oui, une obligation de « protection des renseignements personnels dès la conception » devrait-elle être adoptée comme un principe directeur, une règle sous-jacente ailleurs dans la loi, ou une directive de nature politique?

Q.1(e) : Serait-il logique que la conformité au principe de « protection des renseignements personnels dès la conception » soit aussi assujettie au principe de raisonnabilité et de proportionnalité? Autrement dit, se pourrait-il que l'obligation d'assurer une protection maximale des renseignements personnels ne soit pas absolument nécessaire lorsqu'une solution de rechange raisonnable et proportionnée peut être adoptée à la lumière d'un vaste ensemble de considérations?

3. Sécurité des données

TOUTE INSTITUTION FÉDÉRALE DOIT METTRE EN ŒUVRE DES MESURES TECHNIQUES, ADMINISTRATIVES ET ORGANISATIONNELLES DE SÉCURITÉ DES DONNÉES APPROPRIÉES COMPTE TENU DE LA SENSIBILITÉ DES RENSEIGNEMENTS PERSONNELS AINSI QUE DES RISQUES LIÉS À L'ACCÈS OU AUX ACTIVITÉS NON AUTORISÉES.

La sécurité des données joue un rôle fondamental dans la protection des individus contre les préjudices que pourraient causer un accès non autorisé à leurs renseignements personnels ou une utilisation inappropriée de ces renseignements. Bien que le gouvernement fédéral dispose de politiques sur la sécurité des données, la *Loi sur la protection des renseignements personnels* est elle-même muette sur la question. Il existe cependant certains instruments juridiques – dont le *Règlement général sur la protection des données* (RGPD) de l'Union européenne – qui intègrent des principes visant à assurer la protection adéquate des renseignements personnels, de façon à préserver l'intégrité et la confidentialité de ces renseignements. Le rapport du comité ETHI a aussi recommandé que la *Loi* intègre un principe en ce sens, et qu'elle oblige expressément les institutions à protéger les renseignements personnels en prenant les « mesures physiques, organisationnelles et technologiques convenant au niveau de sensibilité des données. »

Le principe de « sécurité des données » comporte l'obligation de prendre les mesures de sécurité appropriées, de sorte que les institutions doivent régulièrement revoir et améliorer leurs mesures pour les adapter aux nouvelles technologies et aux nouveaux risques qui apparaissent au fil du temps. Les institutions fédérales devraient mettre en œuvre des mesures de sécurité adaptées au contexte, ce qui implique que la rigueur de ces mesures dépendrait du niveau de risque et de la nature des renseignements personnels concernés.

Quand la *Loi sur la protection des renseignements personnels* est entrée en vigueur, en 1983, nous vivions dans un monde où les données étaient conservées sur papier, où le stockage cloisonné de l'information

contribuait à protéger les renseignements personnels, et où l'on ne pouvait même pas imaginer le pouvoir qu'auraient les technologies numériques modernes. Or, ces technologies numériques offrent de nouveaux mécanismes et de nouveaux moyens pour assurer la sécurité des renseignements personnels.

Q.1(f) : Quelles obligations en matière de sécurité des données permettraient aux Canadiennes et Canadiens de se fier à l'intégrité, l'authencité et la sécurité de services gouvernementaux qu'ils emploient, et de se contenter que leurs renseignements personnels soient sécurisés?

Q.1(g) : La *Loi sur la protection des renseignements personnels devrait-elle intégrer un principe fondé sur les mesures de sécurité qui serait similaire à celui de la LPRPDE, afin de faciliter l'interopérabilité dans un contexte contractuel? Y a-t-il d'autres modèles à envisager?*

Q.1(h) : Des règles juridiques particulières devraient-elles être adoptées pour compléter ou renforcer le principe de sécurité, ou devrait-on favoriser l'adoption de solutions propres à chaque institution?

Q.1(i) : Comment pourrait-on tirer parti des nouvelles technologies pour protéger les renseignements personnels?

4. *Ouverture et transparence*

TOUTE INSTITUTION FÉDÉRALE DEVRAIT AVOIR DES PRATIQUES OUVERTES ET TRANSPARENTES EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS ET VEILLER À CE QUE L'INFORMATION APPROPRIÉE SOIT PUBLIQUEMENT DISPONIBLE, DANS DES FORMATS CLAIRS, ACCESSIBLES ET AXÉS SUR LA PRESTATION DE SERVICES.

L'ouverture et la transparence sont des éléments cruciaux de tout instrument législatif moderne de protection des renseignements personnels applicable aux organisations du secteur public, y compris le RGPD. La transparence constitue un élément fondamental des bonnes pratiques de protection des renseignements personnels. Elle aide les institutions à rendre compte, permet aux personnes d'exercer leurs droits et de faire des choix utiles, et peut contribuer à inspirer confiance. D'ailleurs, l'accroissement de la transparence faisait partie des principaux éléments du rapport du comité ETHI concernant la révision de la *Loi sur la protection des renseignements personnels*, qui recommandait que la *Loi* intègre un principe d'ouverture.

Cependant, la transparence ne permet pas à elle seule de susciter une ouverture suffisante : l'information disponible doit aussi être communiquée d'une façon aisément compréhensible. Le principe d'« ouverture et transparence » devrait normalement exiger une transparence significative et encourager l'usage de méthodes créatives et de nouvelles technologies pour organiser, afficher et diffuser de l'information à propos des pratiques concernant les renseignements personnels, de façon à assurer une meilleure communication avec les individus. Les institutions fédérales seraient censées indiquer ouvertement et directement comment elles traitent les renseignements personnels, en faisant preuve de transparence en ce qui concerne : les fins auxquelles ces renseignements sont recueillis, utilisés, conservés ou communiqués; les sources d'orientations qui les guident; la nature des activités automatisées, incluant les systèmes qui recueillent des renseignements personnels; et la façon dont les pratiques de protection des renseignements personnels sont gérées.

Q.1(j) : Une approche fondée sur les principes permettrait-elle de promouvoir l'ouverture et la transparence? Des règles juridiques particulières seraient-elles requises, le cas échéant, pour donner effet à ces objectifs?

Q.1(k) : Quels sont les facteurs pertinents que les institutions doivent prendre en compte pour déterminer comment faire connaître leurs pratiques relatives aux renseignements personnels?

Au moment de songer au principe d'ouverture et de transparence ainsi qu'aux questions connexes, il peut être utile de consulter le document de discussion intitulé *Transparence et responsabilisation : Démontrer l'engagement et le respect nécessaires pour inspirer confiance*.

5. *Responsabilisation*

TOUTE INSTITUTION FÉDÉRALE DOIT ASSUMER SES RESPONSABILITÉS À L'ÉGARD DES RENSEIGNEMENTS PERSONNELS QUI RELÈVENT D'ELLE, ET ELLE DOIT DÉMONTRER SA RESPONSABILISATION EN PROCÉDANT DE FAÇON TRANSPARENTE ET RÉGULIÈRE À LA RÉVISION ET À L'AMÉLIORATION DE SES PRATIQUES EN LA MATIÈRE.

La responsabilisation démontrable est devenue une pratique exemplaire de plus en plus répandue, et elle constitue le fondement de nombreux régimes de protection des données[4]. Le rapport du comité ETHI concernant la révision de la *Loi sur la protection des renseignements personnels* recommandait que la *Loi* intègre un principe de responsabilisation. Selon le principe de responsabilisation démontrable, les institutions auraient la responsabilité de prendre des mesures proactives pour se conformer à la *Loi sur la protection des renseignements personnels* et pour démontrer régulièrement au public et au commissaire à la protection de la vie privée qu'elles respectent la loi. Les institutions ne pourraient pas simplement s'appuyer sur des pratiques connues seulement à l'interne, ou attendre qu'il y ait une plainte ou une enquête avant d'agir : elles seraient tenues de procéder activement à la révision interne de leurs propres pratiques, en toute transparence, puis de les mettre à jour ou de les améliorer au besoin. Le principe de « responsabilisation » permettrait aussi de confirmer le respect continu des exigences à l'égard de la protection des renseignements personnels, tant et aussi longtemps que ces renseignements relèveraient de l'institution.

Q.1(l) : Une approche fondée sur les principes permettrait-elle promouvoir efficacement la transparence? Des règles juridiques particulières seraient-elles requises, le cas échéant, en guise de complément au principe de responsabilisation?

Q.1(m) : Dans le contexte du secteur public fédéral, quelle forme prend la responsabilisation gouvernementale en ce qui concerne les pratiques relatives aux renseignements personnels? Les concepts et exigences qui ont été élaborés à l'intention du secteur privé sont-ils pertinents? Sont-ils adéquats? Sont-ils suffisants?

Au moment de songer au principe d'ouverture et de transparence ainsi qu'aux questions connexes, il peut être utile de consulter le document de discussion intitulé *Transparence et responsabilisation : Démontrer l'engagement et le respect nécessaires pour inspirer confiance.*

B. Application de nouveaux principes de protection des renseignements personnels et de règles modernisées

La question clé est celle de savoir comment les nouveaux principes de protection des renseignements personnels devraient interagir avec la version modernisée des règles actuelles,

Selon les principes cités en exemple dans le présent document, les institutions fédérales seraient censées respecter *à la fois* les règles modernisées et les principes de protection des renseignements personnels proposés.

[4] Voir par exemple la version révisée (en anglais seulement) des *Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel* de l'Organisation de coopération et de développement économique (OCDE), le cadre relatif à la protection des renseignements personnels (*Privacy Framework*) du Forum de coopération économique Asie-Pacifique (APEC), la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (STE nº 108) du Conseil de l'Europe, et le *Règlement général sur la protection des données* (RGPD) de l'Union européenne.

Les règles et les principes joueraient des rôles très différents. D'un côté, les règles continueraient de déterminer *dans quels cas* précis un traitement de renseignements personnels – p. ex. la collecte, la conservation, le maintien de leur exactitude, leur utilisation et leur communication, est spécifiquement autorisé ou exigé De l'autre côté, les nouveaux principes aideraient les institutions à déterminer *comment* exercer ces autorisations ou respecter les exigences en la matière (p. ex. ouvertement, selon des mesures raisonnables et proportionnées, en assurant rigoureusement la sécurité des données, etc.).

Cependant, lorsqu'on cherche à concevoir des règles pour l'avenir, il n'est pas toujours évident de savoir quels genres de technologies existeront, ni quelle sera la nature des risques en matière de protection des renseignements personnels, ni comment les activités des institutions fédérales pourraient évoluer. Puisqu'on ne peut pas prévoir des règles précises pour tous les scénarios possibles, il est utile de songer au rôle que les principes pourraient jouer dans l'autorisation de pratiques inhabituelles ou innovatrices qui sont dans l'intérêt public, mais qui n'avaient pas été prévues lorsque les règles ont été rédigées. Certains ressorts permettent déjà ce genre d'adaptabilité juridique en reconnaissant des situations où des considérations d'intérêt public pourraient l'emporter sur la nécessité de respecter des règles particulières.

Par exemple, la loi australienne (*Privacy Act 1988*) permet au commissaire à la vie privée de faire exception aux règles, s'il le juge dans l'intérêt public, en prenant une décision qui [TRADUCTION] « consiste à déterminer que tel acte ou telle pratique d'une agence ou d'une organisation ne doit pas être considéré comme une atteinte au principe de protection des renseignements personnels, au principe de protection des renseignements de l'État ou à un code approuvé en la matière, alors que cela constituerait autrement une atteinte au principe ou au code concerné ».

Dans le contexte de la protection des données, d'autres États explorent le concept de « bacs à sable réglementaires », qui constituent essentiellement des environnements contrôlés et supervisés où l'on peut mettre à l'essai des modèles de fonctionnement, des structures ou des processus pour vérifier leur conformité avec un ou plusieurs régimes juridiques donnés.

La commissaire à l'information du Royaume-Uni est en train de mettre en œuvre un « bac à sable réglementaire » relatif à la protection des données, aux fins suivantes : soutenir l'utilisation de renseignements personnels pour la prestation de services innovateurs qui sont dans l'intérêt public; assurer une compréhension commune de ce qu'implique le respect des exigences dans des domaines particulièrement innovateurs; et favoriser la réalisation d'une économie de l'innovation. L'atteinte de ces finalités se fera conformément aux paramètres du *Règlement général sur la protection des données* et au droit national[5].

Q.1(n) : Quels sont les rôles les plus importants que devraient jouer les principes de protection des renseignements personnels s'ils étaient intégrés à la Loi sur la protection des renseignements personnels*?*

Q.1(o) : Comment la Loi sur la protection des renseignements pourrait-elle encourager et réglementer efficacement les pratiques inhabituelles ou innovatrices qui n'auraient pas été expressément autorisées par les règles législatives?

[5] https://ico.org.uk/media/about-the-ico/documents/2614219/sandbox-discussion-paper-20190130.pdf

C. Modernisation des règles pour répondre aux attentes raisonnables des individus à l'ère numérique

Les règles établies par la *Loi* actuelle étaient inspirées des principes originaux de l'OCDE quant aux pratiques équitables en matière de protection des renseignements personnels. Il y a cependant des lacunes dans la façon dont les principes de l'OCDE ont été intégrés à la *Loi sur la protection des renseignements personnels*. Les principes originaux de l'OCDE ont d'ailleurs été mis à jour en 2013. Aussi, plus le temps passe, plus il devient justifié de se demander comment les règles canadiennes pourraient être mises à jour pour que nous puissions tirer parti des nouvelles occasions et perspectives optimistes qui se présentent, tout en relevant les nouveaux défis et en répondant aux préoccupations qu'amène la transformation numérique.

Évolution du contexte de l'information

La *Loi sur la protection des renseignements personnels* régit la façon dont le gouvernement traite les renseignements personnels, principalement au moyen des règles énoncées à ses articles 4 à 8. Ces règles n'ont pas été modernisées depuis leur entrée en vigueur en 1983. Elles reflètent donc certaines réalités dépassées en ce qui concerne la circulation de l'information régie par la *Loi sur la protection des renseignements personnels*. Par exemple, au moment où ces règles ont été conçues, on tenait pour acquis que, par défaut, les renseignements personnels ont un cycle de vie linéaire qui commence par leur collecte directe et connue de l'individu, dans le cadre de ses interactions avec l'institution fédérale concernée. Quant à l'obligation de conserver ces renseignements pendant une période minimale prescrite par la loi, elle découle de l'idée que les institutions fédérales risqueraient autrement d'être trop pressées de les éliminer, avant que les individus puissent exercer leur droit d'accès aux renseignements qui les concernent. Par ailleurs, la *Loi* ne traite pas de la question des mesures de sécurité, peut-être parce que l'accent était surtout mis sur la sécurité physique et matérielle des bâtiments.

Évidemment, le contexte dans lequel s'effectue le traitement des renseignements personnels a connu de profondes transformations depuis 1983. L'interaction humaine n'est maintenant plus nécessaire pour que des renseignements personnels soient créés, recueillis, analysés et communiqués. La plupart des institutions ne sont pas pressées de se débarrasser des renseignements personnels dont elles disposent, étant donné les façons concrètes ou potentielles dont les données peuvent contribuer à éclairer la prise de décisions pour relever des défis complexes en matière de politiques publiques. Par exemple, les données peuvent servir à déterminer : dans quelle mesure un programme particulier profite ou non aux différentes populations, et quelles populations se distinguent des autres à cet égard; si une activité gouvernementale donne les effets attendus ou a des conséquences imprévues; ou s'il y a un nouveau problème auquel le gouvernement pourrait ou devrait s'attaquer. En outre, on peut raisonnablement soutenir que la sécurité des données numériques est aujourd'hui beaucoup plus déterminante que les questions de sécurité matérielle de l'information. Et ce ne sont que quelques exemples de changements majeurs qui se sont produits dans le monde de l'information.

Évolution de la façon dont les institutions fédérales remplissent leurs fonctions

Nos règles actuelles sont aussi fondées sur un certain nombre de perspectives dépassées quant au rôle du gouvernement et aux façons dont les institutions fédérales remplissent leurs fonctions et interagissent avec les gens et le public en général.

Lorsque la *Loi sur la protection des renseignements personnels* est entrée en vigueur, en 1983, le stockage des renseignements de façon cloisonnée faisait partie des moyens pertinents de préserver la vie privée. À cette époque, on ne pouvait même pas imaginer tout le potentiel des technologies numériques modernes et le pouvoir qu'elles finiraient par receler. De nos jours, les institutions fédérales collaborent entre elles pour exercer leurs fonctions publiques – qu'il s'agisse de fournir des services au public, de réglementer un secteur d'activité particulier ou d'assurer l'administration ou l'application des lois – et les technologies numériques offrent des occasions d'innovation accrue dans l'intérêt public. Conserver l'information à un seul endroit n'est plus la principale façon de protéger les renseignements personnels. Dans certains cas, sur les plans de la

technologie, de la gouvernance et de l'administration, il peut exister des solutions nouvelles, capables d'assurer une protection équivalente tout en réduisant les contraintes par rapport aux objectifs généraux de politiques publiques. Tandis que l'Internet des objets et les flux de données « ambiants » s'intègrent à la réalité moderne, les institutions ne sont plus forcément en mesure de garder la pleine maîtrise de tous les renseignements personnels qui « relèvent » d'elles. Et il n'est plus évident de savoir si les renseignements personnels accessibles au public devraient toujours être exclus de l'application des règles relatives à l'utilisation et à la communication des renseignements personnels, compte tenu des nouvelles façons dont ils peuvent être utilisés.

Certains des a-priori de la loi concernant la façon dont les institutions fédérales remplissent leurs fonctions ne sont pas conformes aux attentes modernes des individus quant au rôle de ces dernières et aux manières de répondre à leurs besoins individuels et sociaux. En matière de politiques publiques, les défis majeurs, complexes et interreliés que les institutions fédérales doivent relever impliquent ce qui suit : les mesures à prendre doivent être adaptées à une multiplicité d'institutions, de ressorts et d'aspects; les interventions efficaces s'appuient plus que jamais sur les données; et les membres du public s'attendent à obtenir des services cohérents, coordonnés et pratiques en toutes circonstances, à tous les stades de leur vie et dans tous les domaines d'activité, sans se buter à des limites administratives circonscrites de façon étroite. Et parallèlement, de nombreux individus sont de plus en plus soucieux d'obtenir la maîtrise de leurs renseignements personnels, y compris ceux qui sont accessibles au public. Il serait donc utile de mettre à l'épreuve les règles en vigueur, pour remettre en question les perspectives et les considérations qui ne sont plus pertinentes ou justifiées.

Q.1(p): Une révision quinquennale de la Loi permettrait-elle de rester courante face aux changements?

Consentement

Au regard des discussions publiques sur le rôle du consentement dans le traitement des renseignements personnels, voici une question clé à se poser : comment le consentement devrait-il fonctionner dans le contexte du gouvernement et du secteur public?

Dans sa version actuelle, la *Loi sur la protection des renseignements personnels* n'exige pas qu'il y ait consentement pour que des renseignements soient recueillis. Si on choisissait de faire autrement, il faudrait tenir compte d'une exigence fondamentale : pour être jugé valide, le consentement doit être libre et éclairé. Dans le contexte du secteur public, il peut s'avérer très difficile de veiller à ce que le consentement respecte cette exigence essentielle. Certains individus pourraient craindre des conséquences négatives en cas de refus et se sentir obligés de consentir à la collecte de renseignements personnels. La collecte est par conséquent fondée sur le lien avec une activité légale de l'institution fédérale. Cela est conforme à la plupart des lois sur la protection des renseignements personnels applicables au secteur public, de même qu'à l'approche relative aux autorités publiques qui est prévue dans le *Règlement général sur la protection des données* (RGPD) de l'UE.

[TRADUCTION] « On ne peut généralement pas considérer qu'il y a un véritable consentement lorsqu'il existe un déséquilibre manifeste des pouvoirs entre la personne concernée et vous. La raison en est que les personnes qui dépendent de vos services, ou qui craignent des conséquences négatives, peuvent estimer qu'elles n'ont pas le choix d'accepter – alors on ne peut pas considérer que le consentement est donné librement. C'est un problème qui touche particulièrement les autorités publiques et les employeurs[6]. »

[6] Commissariat à l'information du Royaume-Uni (Information Commissioner's Office), *Guide to Data Protection*, « When is consent appropriate? », https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

« Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière[7]. »

On peut aussi s'inquiéter du fait que les modèles fondés sur le consentement peuvent amener des institutions disposant d'importantes ressources à se « décharger » concrètement et indûment d'une importante mesure de responsabilisation et à rejeter cette trop lourde responsabilité sur les individus. On ne peut pas s'attendre à ce que les individus soient toujours en mesure de bien comprendre ce qui est demandé, de remettre les choses en question et de répondre de façon éclairée aux nombreuses demandes de consentement qu'on leur présente au quotidien – et le problème pourrait être particulièrement exacerbé par les déséquilibres de pouvoir inhérents au secteur public.

Dans le secteur public, il existe des solutions de rechange tout à fait valables pour éviter de s'en remettre au consentement. Par exemple, le droit public exige que les institutions publiques s'en tiennent strictement aux activités qui se situent dans les limites du mandat que leur confère la loi. La *Loi sur la protection des renseignements personnels* vient y ajouter une exigence, en faisant en sorte que les institutions peuvent seulement recueillir des renseignements personnels ayant un lien suffisamment direct avec les programmes et activités légalement autorisés au titre de leur mandat. Et le fait qu'une personne consente à fournir des renseignements personnels ne permet pas d'élargir la portée de ce mandat au-delà de ce que l'institution est dûment autorisée à faire. La *Loi* fonctionne donc selon un modèle fondé sur l'autorité ou l'autorisation légale.

Cela dit, la *Loi sur la protection des renseignements personnels* reconnaît la capacité des individus de donner un consentement véritable et valide dans certains cas, y compris pour un usage particulier ou pour la communication de renseignements personnels. Une fois que l'institution fédérale a rempli les exigences établies pour recueillir validement les renseignements demandés, la *Loi* permet à l'individu concerné d'autoriser l'utilisation ou la communication ultérieure en fournissant son consentement à cette fin. Cette façon de faire permet à l'individu d'exercer son autonomie et sa capacité de contrôler l'usage et la communication de ses renseignements personnels dans certaines circonstances.

Q.1(q) : Dans quels contextes la Loi sur la protection des renseignements personnels *devrait-elle permettre aux individus de prendre des décisions éclairées et de donner un consentement valide concernant le traitement de leurs renseignements personnels?*

Q.1(r) : Comment les individus peuvent-ils exercer un contrôle et donner un consentement à l'égard de leurs renseignements personnels sous le modèle de gouvernance de la Loi touchant l'accès légal et l'autorité légale d'accéder aux renseignements personnels?

La question du consentement est aussi traitée dans le document de discussion intitulé *Greater Certainty for Canadians and Government – Delineating the Contours of the Privacy Act and Defining Important Concepts* (Vers une plus grande certitude pour la population canadienne et le gouvernement – recadrage de la *Loi sur la protection des renseignements personnels* et définition de concepts importants).

Collecte

Pour obtenir des renseignements personnels, les institutions fédérales doivent d'abord en faire la collecte. Habituellement, avant de pouvoir recueillir ces renseignements, il faut déterminer à quelles fins ils serviront et veiller au respect des conditions préalables. L'article 4 de la *Loi sur la protection des renseignements*

[7] RGPD, considérant 43, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32016R0679

personnels régit la collecte des renseignements personnels. Aux termes de cet article, « [l]es seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ». Autrement dit, il est interdit de recueillir des renseignements personnels qui ne sont pas fondamentalement requis pour l'exécution du programme ou de l'activité pour laquelle la collecte est effectuée.

Cette approche est fondée sur la conception selon laquelle le gouvernement se compose de ministères qui travaillent chacun de façon isolée, sans collaborer à l'atteinte d'objectifs communs. Elle est aussi rattachée à l'idée qu'une protection efficace des renseignements personnels exige une compartimentation étroite de l'information selon les seules fins du programme ou de l'activité en question. Or, pour être efficaces, les programmes gouvernementaux et les ministères collaborent de plus en plus les uns avec les autres pour éviter la répétition inutile des mêmes efforts et optimiser les interactions avec les individus. Aux yeux de bon nombre d'individus, ce qui compte le plus est d'assurer l'efficacité du processus – que ce soit pour obtenir des prestations, demander un permis ou informer le gouvernement d'un événement important de la vie –, et non de savoir quel ministère joue quel rôle particulier et quel programme ministériel entre en jeu.

En concevant des dispositions portant sur la collecte d'information, notre objectif est de réduire le plus possible les répercussions sur la protection des renseignements personnels. Dans cette perspective, nous devons songer à la façon de baliser le pouvoir de collecte dans le contexte d'une loi-cadre adaptée à la société moderne.

Seuil justifiant la collecte

Un des enjeux importants consiste à déterminer les conditions que les institutions fédérales doivent respecter pour être autorisées à recueillir des renseignements personnels. Peu importe le critère utilisé, les conditions doivent être applicables à l'ensemble des rôles confiés aux institutions fédérales, qui peuvent aller de la prestation de services à la réalisation de recherches et à l'obtention de statistiques, en passant par l'analyse des politiques, la réglementation et l'exécution de la loi.

Certains intervenants jugent trop permissif le critère actuel d'autorisation de la collecte – à savoir que les renseignements personnels recueillis doivent être directement liés au programme ou à l'activité de l'institution fédérale concernée.

Préoccupé par le risque de collecte excessive – qui est exacerbé par la facilité de circulation des données dans l'environnement numérique actuel –, le commissaire à la protection de la vie privée a recommandé que l'on modifie la *Loi sur la protection des renseignements personnels* pour y inclure le critère de la « nécessité » comme seuil justifiant la collecte. Dans son témoignage devant le comité ETHI, le 22 mars 2016, il a soutenu que, pour respecter ce critère de la nécessité, l'institution concernée aurait à s'assurer que « l'information a un lien rationnel avec ses programmes ou ses activités et est manifestement nécessaire pour ces derniers ». À cet égard, la question de la nécessité manifeste serait déterminée selon le cadre d'analyse énoncé dans l'arrêt *Oakes* :

> « (…) les renseignements personnels seraient recueillis conformément au critère de la nécessité si l'information a un lien rationnel avec ses programmes ou ses activités et est manifestement nécessaire pour ces derniers; s'il est probable qu'elle répondrait de façon efficace aux objectifs du programme ou de l'activité; qu'il n'y a aucun autre moyen d'atteindre efficacement les objectifs du programme ou de l'activité en portant moins atteinte à la vie privée; et si la perte de vie privée est proportionnelle à l'importance des objectifs du programme ou de l'activité[8]. »

[8] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2016/parl_sub_160322/

Dans le cadre de l'étude du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (comité ETHI) à propos de la révision de la *Loi sur la protection des renseignements personnels*, certains témoins ont quant à eux exprimé l'idée que la proportionnalité pourrait représenter un seuil approprié. L'un des témoins a formulé la question ainsi : « L'avantage pour le fonctionnement du gouvernement ou le pays dans son ensemble est-il proportionnel à tout compromis en matière de protection des renseignements personnels? Je pense que ce sont des questions qu'on devrait régulièrement poser. » Dans son rapport de décembre 2016, *Protéger la vie privée des Canadiens : Examen de la Loi sur la protection des renseignements personnels,* le comité ETHI a recommandé que la norme relative à la collecte de données tienne compte à la fois de la nécessité et de la proportionnalité.

Il va sans dire que l'effet de l'introduction d'un critère de nécessité dans la *Loi* serait tributaire de la définition du concept de nécessité et de la façon dont elle serait déterminée concrètement, selon la situation.

À cet égard, l'incertitude demeure sur au moins deux aspects. La première question consiste à déterminer comment faire la distinction entre, d'une part, la « nécessité absolue », qu'aucun intervenant ne semble privilégier, et, d'autre part, la « nécessité raisonnable ou manifeste ». La deuxième question est celle de savoir à quoi, au juste, les renseignements personnels devraient être nécessaires. En théorie, plus le seuil est élevé, moins les institutions fédérales seraient censées pouvoir recueillir des renseignements. En pratique, cela dépendrait à la fois de la façon dont le seuil est déterminé et de la portée du programme ou de l'activité que vise la collecte. Par exemple, les renseignements nécessaires pour évaluer l'admissibilité d'un individu à un programme peuvent être plus limités que ceux nécessaires pour évaluer l'efficacité du programme ou son succès auprès de différents groupes démographiques, ou encore pour effectuer des recherches sur les facteurs sociaux déterminants.

Recueillir seulement les renseignements personnels nécessaires est reconnu depuis longtemps comme un moyen exemplaire de limiter les répercussions et les risques en matière de protection des renseignements personnels. Cependant, c'est le résultat qui importe – à savoir la limitation des répercussions sur la protection des renseignements personnels –, et non dans la façon de l'obtenir. Dans certains cas, il peut arriver que la meilleure façon de protéger les renseignements personnels ne consiste pas à restreindre au strict minimum la quantité d'information recueillie et communiquée. Cette approche pourrait même nuire à l'atteinte d'importants objectifs d'intérêt public, notamment le soutien d'interventions éclairées en matière de politiques, au moyen d'éléments probants, et l'obtention des renseignements requis pour éviter un manque de données globales qui pourrait s'avérer néfaste à grande échelle. Cela pourrait aussi empêcher ou retarder des enquêtes que doivent mener les organismes d'application de la loi, en soulevant des questions concernant la réelle « nécessité », pour l'enquête en question ou le mandat législatif à remplir, de recueillir des renseignements au moyen d'une technique d'enquête donnée. Un critère de nécessité – qui vient essentiellement imposer un moyen particulier et prescriptif de respecter l'objectif d'« atteinte minimale » – peut aussi contraster avec le fait que bon nombre d'individus ne voient pas vraiment de problème à ce que leurs renseignements personnels soient utilisés dans l'intérêt public, même si ce n'est pas absolument « nécessaire », à condition que des mesures soient prises pour atténuer les répercussions et les risques en matière de protection des renseignements personnels, et que les responsables fassent preuve de transparence dans la façon de protéger, d'analyser et d'utiliser ces renseignements.

Ultimement, le concept de « nécessité » prête largement à interprétation. Il est donc essentiel que la *Loi sur la protection des renseignements personnels* précise clairement à quelles fins la collecte de renseignements personnels pourrait être « nécessaire ». L'objectif doit-il se limiter strictement à la mise en œuvre d'un programme? Ou le critère de nécessité offre-t-il une certaine latitude pour recueillir des renseignements dans le but d'assurer l'efficacité de cette mise en œuvre, conformément aux obligations et engagements généraux du gouvernement?

En outre, plutôt que d'utiliser l'expression « ses programmes ou ses activités », il pourrait être préférable de faire plus généralement référence à la collecte de renseignements personnels à des fins déterminées,

explicites et légitimes, que la loi autoriserait vraisemblablement pour des autorités publiques. Par exemple, aux termes du RGPD de l'UE, les autorités publiques sont autorisées à traiter des données à caractère personnel lorsque c'est nécessaire « à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (article 6). Cela évite de s'attarder aux divisions administratives au sein même de l'institution concernée.

Q.1(s) : Comment est-ce que l'approche concernant la collecte de renseignements aux termes de la Loi sur la protection des renseignements personnels peut être modelée afin d'être suffisamment fondée sur les principes, flexible et claire, de façon à offrir une protection robuste des renseignements personnels sans pour autant compromettre ce à quoi les individus et le public s'attendent du gouvernement?

Q.1(t) : Est-ce que différentes approches s'imposent selon le contexte? Par exemple, des règles spécifiques seraient-elles requises pour offrir des directives relatives à la collecte de renseignements personnels disponibles publiquement sur Internet et sur les médias sociaux?

Q.1(u) : À quoi le critère de collecte devrait-il être lié? Plus précisément, est-ce que le critère relatif à la collecte devrait être lié : aux fins d'un programme ou d'une activité en particulier; à un objectif d'intérêt public qui est légitime ou autorisé; au mandat et aux fonctions d'une institution fédérale; ou à quelque chose d'autre?

Q.1(v) : Si le principe de raisonnabilité et de proportionnalité s'appliquait à la collecte, un critère de nécessité serait-il néanmoins utile?

Autres considérations en matière de collecte

À la lumière de l'expérience passée des institutions fédérales relativement à la *Loi sur la protection des renseignements personnels*, d'autres questions méritent d'être considérées.

Premièrement, le fait de régir la collecte à l'échelle particulière d'un programme ou d'une activité *propre à une institution donnée* n'est pas toujours cohérent avec les modes de fonctionnement modernes du gouvernement et avec les façons dont les Canadiennes et les Canadiens s'attendent à être servis. Si une institution fédérale peut seulement recueillir les renseignements personnels nécessaires à ses propres programmes, elle ne sera peut-être pas en mesure d'adopter des approches intégrées et plus efficaces pour la prestation de services publics qui recoupent ceux d'autres institutions ou qui y sont liées.

Deuxièmement, puisque la nature, le format et le mode de circulation des renseignements personnels ont évolué, ces renseignements pourraient être involontairement recueillis de façon non conforme à la *Loi*, s'ils sont obtenus de façon non sollicitée ou par des moyens passifs. Pour ce genre de situation, la *Loi* ne fournit aucune ligne directrice et ne prévoit aucune exception. Par exemple, le fonctionnement de nouvelles technologies « grand public », notamment dans les véhicules autonomes, pourrait intrinsèquement reposer sur la collecte de renseignements personnels – relativement aux passagers, aux piétons et aux autres conducteurs – dont la portée dépasserait ce que les institutions veulent ou doivent obtenir pour remplir leur mandat. Plutôt que d'en faire une violation des règles de collecte, la nouvelle *Loi* pourrait préciser ce que l'on doit faire de ces renseignements recueillis involontairement : comment déterminer s'il vaut mieux les détruire ou les conserver?

Troisièmement, la collecte directe représente une importante mesure de transparence, de responsabilisation et de protection. Selon la règle établie en la matière, les institutions fédérales doivent, dans la mesure du possible, recueillir directement auprès de l'individu concerné les renseignements personnels à utiliser pour la prise de décisions le concernant. Des exceptions sont autorisées dans les cas où l'individu a consenti à la collecte indirecte de ces renseignements, ou si une autre institution est autorisée à les communiquer à l'institution qui en a besoin. Cependant, les exigences actuelles de collecte directe pourraient être difficiles à

maintenir, compte tenu des nouveaux modes de création et de circulation des renseignements personnels (p. ex. les flux de données « ambiants » générés par des capteurs). De plus, certains individus ne souhaitent pas nécessairement que l'on s'adresse à eux directement dans chaque situation.

Q.1(w) : L'ajout de nouvelles exigences de responsabilisation et de transparence pourrait-il constituer, dans certaines circonstances, une solution de rechange à la collecte directe?

Q.1(x) : Dans quelles circonstances la notification pourrait-elle constituer une solution de rechange à la collecte directe?

Conservation

Le paragraphe 6(1) de la *Loi sur la protection des renseignements personnels* exige que les institutions fédérales conservent, pendant une période déterminée par règlement, les renseignements personnels qui ont été utilisés à des fins administratives. Cela vise à accorder une période « suffisamment longue pour permettre à l'individu qu'ils concernent d'exercer son droit d'accès à ces renseignements ». Le règlement pris en vertu de la *Loi sur la protection des renseignements personnels* a établi la norme de conservation à « au moins deux ans » après la dernière utilisation des renseignements en question dans le cadre d'une décision touchant directement la personne, à moins que celle-ci consente à devancer leur disposition.

Ces règles de conservation, très prescriptives et centralisatrices, n'offrent aucune souplesse d'adaptation au contexte. Elles imposent une période de conservation minimale sans préciser de critères qui permettraient de déterminer une échéance de disposition plus appropriée. Cela découle de l'importance fondamentale accordée au droit d'accès aux renseignements personnels, et de l'objectif explicite qui consiste à donner une occasion suffisante d'exercer ce droit, particulièrement dans le cas de renseignements qui ont été utilisés dans le cadre de décisions touchant directement l'individu.

Si cette approche est conçue pour protéger efficacement le droit d'accès, elle n'est toutefois pas conforme aux pratiques exemplaires visant à limiter le stockage de renseignements personnels et à disposer de ceux qui ne sont plus nécessaires. La règle actuelle exigeant leur conservation pendant deux ans n'est pas adaptable aux situations où la vie privée serait mieux protégée par une disposition rapide des renseignements personnels après leur utilisation.

À l'ère numérique, lorsque les renseignements personnels ne sont plus utiles aux fins pour lesquelles ils ont été recueillis, le fait de les conserver plus longtemps peut mettre leur protection en péril, et ainsi représenter un risque plus important que celui de faire obstacle au droit d'accès. En contrepartie, il se pourrait que ces renseignements aient plus tard une autre utilité d'intérêt public, ce qui pourrait justifier une approche prudente quant à leur disposition.

L'importance du droit d'accès et des pratiques de disposition prudentes ressort de façon particulièrement claire lorsque les renseignements personnels ont été recueillis indirectement. Dans ces situations, l'individu ne sait pas nécessairement quels renseignements le concernant ont été recueillis, ni pourquoi et comment ils ont pu servir à prendre des décisions à son sujet. Dans ce genre de cas, il y aurait peut-être lieu de privilégier la protection du droit d'accès. Par contre, lorsque l'individu a fourni sciemment et directement ses renseignements à un décideur gouvernemental à des fins déterminées, des pratiques prudentes de dispositions rapides sembleraient davantage justifiées.
Compte tenu des considérations qui précèdent, il y aurait probablement lieu de rééquilibrer l'approche de conservation actuelle afin d'améliorer les possibilités d'adaptation au contexte.

Q.1(y) : Comme certains l'ont proposé devant le comité ETHI, est-ce qu'un critère de proportionnalité représenterait un moyen viable de passer à une approche de conservation plus souple, fondée sur des principes?

Q.1(z) : Y a-t-il des critères particuliers qui devraient guider les décisions en matière de conservation des renseignements personnels?

Exactitude

Le paragraphe 6(2) de la *Loi sur la protection des renseignements personnels* énonce l'obligation des institutions fédérales d'assurer l'exactitude des renseignements personnels qui relèvent d'elles. Il est axé sur le résultat et formulé comme un principe. Il énonce l'obligation ainsi : « Une institution fédérale est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels qu'elle utilise à des fins administratives soient à jour, exacts et complets. » Ce paragraphe reflète assez bien le principe de la qualité des données établi par l'OCDE.

Le rapport de 2016 du comité ETHI ne traite pas de façon très détaillée la question de l'exactitude des renseignements personnels. Cependant, on y note le point de vue d'un témoin, selon lequel cette obligation d'assurer l'exactitude des renseignements personnels devrait aller au-delà des fins administratives et s'appliquer à tout renseignement personnel, peu importe les fins pour lesquelles il est utilisé ou communiqué. Selon ce témoin, les renseignements inexacts peuvent avoir de graves conséquences au regard des droits et des libertés fondamentales de la personne.

Au Canada, c'est la *Loi canadienne sur les droits de la personne* qui a énoncé les premières règles législatives régissant la protection des renseignements personnels dans le secteur public fédéral. Encore aujourd'hui, il y a des liens étroits et manifestes entre le droit à la protection des renseignements personnels et plusieurs autres droits, particulièrement les droits à l'égalité, à l'autonomie et à la dignité humaine. C'est une considération historique utile à prendre en compte pour la révision de l'obligation d'exactitude. Le fait est que d'importantes préoccupations commencent à se manifester par rapport aux systèmes axés sur les données, qui ont désormais le potentiel d'apprendre par eux-mêmes et de renforcer les tendances à la discrimination et à l'exclusion, et de soumettre les individus et leurs intérêts fondamentaux à de nouveaux risques, dont certains sont encore inconnus. Les préoccupations du public sont devenues manifestes à cet égard, comme en témoigne le fait que, dans le discours public, on entend de plus en plus parler des risques que représentent les décisions automatisées, fondées sur des algorithmes. Ces préoccupations sont étroitement liées aux questions d'exactitude et d'intégrité des données, mais elles concernent aussi les principes généraux en matière d'éthique et de lutte à la discrimination.

Q.1(aa) : Quel rôle devrait jouer la Loi sur la protection des renseignements personnels *en réponse aux préoccupations concernant les droits de la personne et les enjeux éthiques découlant de l'utilisation de nouveaux outils analytiques et de processus de décision automatisés?*

Q.1(bb) : L'obligation d'exactitude énoncée dans la loi permet-elle d'atténuer suffisamment les multiples risques que les systèmes axés sur les données représentent pour les individus? Devrait-on revoir ses paramètres en fonction de la transformation numérique?

Usage et communication

Les articles 7 et 8 de la *Loi sur la protection des renseignements personnels* régissent l'utilisation et la communication des renseignements personnels par les institutions fédérales. Ces articles établissent un

équilibre entre, d'une part, l'importance fondamentale de protéger les renseignements personnels et, d'autre part, la nécessité de permettre l'utilisation et la communication responsables de renseignements personnels dans l'intérêt public. Treize scénarios permettant l'usage et la communication de renseignements personnels sans consentement sont reconnus. Chacun d'eux est établi selon les fins auxquelles l'usage ou la communication des renseignements doit servir, et certains sont conditionnels à des mesures de protection et à des mécanismes de responsabilisation propres au contexte.

Aux termes de la *Loi*, les renseignements personnels peuvent être communiqués ou utilisés aux fins suivantes : celles pour lesquelles ils ont été recueillis, les usages compatibles avec ces fins; les fins conformes à une loi ou un règlement; la conformité aux règles de procédure; la facilitation du rôle du procureur général en matière de contentieux; la tenue d'enquêtes ou le respect des lois; l'application d'ententes de communication de renseignements qui contribuent à la bonne administration de la loi; l'aide aux citoyens par l'intermédiaire d'un député; l'établissement des droits des peuples autochtones ou du règlement de leurs griefs à l'égard de la Couronne; le recouvrement de dettes; et dans les cas où leur utilisation ou leur communication serait justifiée par des raisons « d'intérêt public ».

Étant donné l'évolution du contexte général depuis l'adoption de la Loi, certaines dispositions sont-elles devenues superflues?

Q.1(cc) : Les fins justifiant l'utilisation et la communication de renseignements personnels sont-elles encore conformes aux attentes raisonnables des individus quant à la façon dont les institutions fédérales devraient les utiliser et les communiquer?

Après plus de 35 ans d'usage, dans quelle mesure et de quelle façon les dispositions actuelles devraient-elles être modernisées pour tenir compte de l'évolution du contexte dans lequel elles trouvent application?

Q.1(dd) : Quelles dispositions relatives à l'usage et à la communication de renseignements personnels exigent que des mesures de protection et des mécanismes de transparence et de responsabilisation supplémentaires soient prévus? De nombreux intervenants ont donné comme exemple les ententes de communication de renseignements. Y a-t-il d'autres exemples?

Q.1(ee) : Pour ce qui est des ententes de partage de renseignements personnels, les échanges vers l'étranger devraient-ils être traités différemment des échanges au domestique? Les institutions fédérales devraient-elles faire mesure de transparence à l'égard de l'existence des ententes d'échange de renseignements personnels, et de les publier? Si oui, dans quelles circonstances des exceptions à cette obligation seraient appropriées?

Plusieurs de ces dispositions comportent une certaine souplesse quant à leur portée et à leur application. Il pourrait difficilement en être autrement, puisqu'il s'agit d'un cadre législatif qui s'applique de façon générale à plus de 250 institutions fédérales ayant chacune son propre mandat, ses besoins spécifiques d'information et ses propres partenariats avec des organismes d'autres ressorts. Certains pourraient par conséquent soutenir qu'il n'est pas nécessaire d'ajouter des scénarios permettant l'usage et la communication de renseignements personnels dans d'autres circonstances. Toutefois, après plus de 35 ans d'application, on peut facilement concevoir qu'il existe certaines lacunes – ou à tout le moins un besoin de clarification.

Par exemple, des modifications pourraient permettre aux Canadiennes et Canadiens de bénéficier d'une approche « une fois suffit », de façon à ce que des renseignements clés ne soient recueillis qu'une seule fois et partagé avec d'autres ministères et agences ayant besoin ces renseignements afin d'offrir un bénéfice ou un service. Ceci pourrait se faire :

- En assurant que les renseignements personnels sont pertinents, à jour et exacts entre programmes et services, sans que le client ait à fournir de nouveau les mêmes mises à jour à plusieurs ministères et agences;
- En réutilisant des renseignements préexistants et déjà fournis au Gouvernement du Canada, y compris pour remplir préalablement un formulaire à partir de renseignements déjà entre les mains du gouvernement, afin de simplifier les services pour les Canadiennes et Canadiens, et d'offrir de façon proactive des bénéfices et des services aux clients en réutilisant leurs renseignements.

Permettre davantage de partage de renseignements entre services autorisés, dans des circonstances soigneusement définies, pourrait appliquer des analyses fondées sur la recherche et des statistiques afin d'améliorer la conception et la prestation des services, et pourrait améliorer l'intégrité des programmes (par exemple, afin de prévenir la réception frauduleuse des bénéfices). En se dirigeant vers un plus grand partage de renseignements entre services, assurer que le gouvernement soit transparent à l'égard des renseignements qu'il a entre les mains et comment ils sont utilisés, serait une considération importante.

Q.1(ff) : En général, quels critères seraient utiles pour déterminer les nouvelles situations dans lesquelles l'utilisation et la communication de renseignements personnels devraient être permises?

Q.1(gg) : Où peut-il y avoir des lacunes dans les autorités actuelles permettant l'utilisation et le partage de renseignements personnels? Les Canadiens auraient-ils besoin d'obtenir un meilleur soutien à des étapes particulières de la vie ou dans des situations telles que la mort d'un proche? Pourrait-on faire en sorte que tous les programmes de prestations partagent les renseignements dont ils disposent, de façon à aider les individus et à améliorer l'efficacité des services?

Q.1(hh) : Si le gouvernement était à partager et à utiliser des renseignements personnels entre des fournisseurs de services et de programmes autorisés afin d'améliorer la livraison de services, quels facteurs devrait-on considérer? Quelles mesures de protection et quelles limites devrait-on imposer sur de tels partages et usages de renseignements?

Les fonctions du gouvernement relatives à la sécurité nationale, au renseignement et à l'application de la loi viennent souvent à l'esprit des gens lorsqu'ils pensent à l'utilisation et au partage de renseignements personnels par le gouvernement.

La *Loi sur la protection de renseignements personnels* – y compris le rôle et les pouvoirs du commissaire à la protection de la vie privée – s'applique aux fonctions du gouvernement relatives à la sécurité nationale, au renseignement et à l'application de la loi. Toutefois, la *Loi sur la protection de renseignements personnels* va de pair avec d'autres régimes juridiques spécialisés de ce contexte. À titre d'exemple, des pouvoirs juridiques particuliers sont requis pour que le gouvernent puisse exercer des fonctions en matière de sécurité nationale, de renseignement et d'application de la loi, et ceux-ci sont prévus à des lois comme la *Loi sur le Service canadien du renseignement de sécurité* et la *Loi sur les douanes*, ainsi que la *Loi sur le centre de la sécurité des télécommunications* proposée. Les pouvoirs uniques des forces policières sont assujettis à des mécanismes de protection spécifiques avec une surveillance accrue de la part des tribunaux juridiques, y compris les obligations du *Code criminel* exigeant l'obtention d'un mandat pour des perquisitions et des fouilles. Par ailleurs, il existe d'autres lois spécifiques qui s'appliquent aux échanges de renseignements dans ce contexte.

Q.1(ii) : À la lumière de ce contexte complexe, des modifications aux dispositions permettant l'utilisation et le partage de renseignements personnels prévues à la Loi sur la protection des renseignements personnels sont-elles nécessaires afin d'assurer une mesure d'interopérabilité avec ces régimes?

Accès

À l'heure actuelle, la *Loi sur la protection des renseignements personnels* permet aux citoyens canadiens, aux résidents permanents et aux personnes physiquement présentes au Canada de faire des demandes d'accès aux renseignements personnels les concernant. Le Canada fait quelque peu bande à part en délimitant ainsi les catégories d'individus qui disposent d'un droit d'accès à leurs propres renseignements personnels. La commissaire à l'information a fait remarquer que, parmi un large éventail de ressorts comparables[9], seuls le Canada, la Nouvelle-Zélande et l'Inde imposent ainsi des limites quant aux personnes qui peuvent avoir accès à l'information détenue par le gouvernement.

À cet égard, le comité ETHI recommande que le gouvernement du Canada envisage d'accorder aussi aux ressortissants étrangers le droit d'accès aux renseignements personnels qui les concernent.

Déjà, les ressortissants étrangers qui veulent accéder à leurs renseignements personnels peuvent recourir à la *Loi sur l'accès à l'information*, plutôt qu'à la *Loi sur la protection des renseignements personnels*, et certains le font effectivement, en faisant appel à un agent au Canada et en se servant de la disposition de consentement pour que ces renseignements puissent être communiqués à l'agent en question. De plus, des institutions peuvent traiter les demandes de ressortissants étrangers de façon discrétionnaire, sans passer par l'un ou l'autre des deux régimes.

La circulation mondiale grandissante des renseignements personnels et la récente entrée en vigueur du *Règlement général sur la protection des données* de l'Union européenne soulèvent d'autres considérations importantes. Étant donné l'importance du droit d'accès, le régime actuel du Canada donne lieu à des problèmes d'interopérabilité. Pour reconnaître aux ressortissants étrangers un droit d'accès à leurs renseignements personnels, il ne semble pas particulièrement judicieux ou efficace de s'en remettre à la négociation ponctuelle et individuelle d'ententes.

Cependant, certains témoins ayant comparu devant le comité ETHI ont exprimé des préoccupations quant au fait que l'élargissement du droit d'accès pourrait imposer un fardeau excessif sur les ressources institutionnelles et créer des contraintes opérationnelles. Selon certains, avant d'accorder le droit d'accès aux renseignements personnels à d'autres personnes, il faudrait commencer par améliorer le temps de réponse pour les personnes qui disposent déjà de ce droit. Bien qu'il s'agisse d'une considération importante, il se pourrait aussi que l'utilisation de nouvelles technologies et de nouveaux processus contribue à soulager les pressions qui pèsent sur le système.

Q.1(jj) : Étant donné que l'élargissement du droit d'accès pourrait avoir des implications pratiques incertaines, mais que des raisons convaincantes incitent à l'envisager, l'expérimentation réglementaire pourrait-elle représenter une solution intermédiaire? Par exemple, pourrait-il être utile de recourir à des instruments de politique pour mener un projet pilote accordant un droit d'accès élargi dans certains cas, afin de recueillir des données susceptibles d'éclairer les futurs changements législatifs?

Q.1(kk) : Y a-t-il d'autres aspects stratégiques pertinents à considérer en ce qui concerne l'élargissement du droit d'accès aux renseignements personnels?

[9] https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2016/parl_sub_160322/: « Parmi les provinces et les territoires, les pays du Commonwealth, les États-Unis, dans les lois types et dans les pays dont la loi sur l'accès à l'information se classe parmi les 10 premières selon le "Global Right to Information Rating", le Canada, la Nouvelle-Zélande et l'Inde sont les seuls à imposer des limites quant aux personnes qui peuvent avoir accès à l'information détenue par le gouvernement. Toutes les autres juridictions ont un droit d'accès universel (…) »