



Commissariat
à la protection de
la vie privée du Canada

RÉFORME DES LOIS SUR LA VIE PRIVÉE

POUR FAIRE RESPECTER LES DROITS ET RÉTABLIR LA CONFIANCE
ENVERS LE GOUVERNEMENT ET L'ÉCONOMIE NUMÉRIQUE

2018 • 2019
RAPPORT ANNUEL



**Rapport annuel au Parlement 2018-2019 concernant la *Loi sur la protection des renseignements personnels*
et la *Loi sur la protection des renseignements personnels et les documents électroniques***

Commissariat à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec) K1A 1H3

© Sa Majesté la Reine du chef du Canada pour le Commissariat à la protection de la vie privée du Canada, 2019

Numéro de catalogue : IP51-1F-PDF

ISSN : 1913-3375



Table des matières

Message du commissaire	2	Conseils aux entreprises	54
La protection de la vie privée en chiffres	6	Programme des contributions	55
Conseils au Parlement	7	Devant les tribunaux	56
Réforme des lois sur la protection des renseignements personnels : une voie vers le respect des droits et le rétablissement de la confiance envers le gouvernement et l'économie numérique	8	Coopération avec des autorités canadiennes et étrangères	59
Activités parlementaires	24	Annexe 1 : Définitions	61
La Loi sur la protection des renseignements personnels (LPRP) – Rétrospective de l'exercice ..	29	Annexe 2 : Tableaux statistiques	64
Mises à jour et tendances en matière de fonctionnement	30	Tableaux relatifs à la LPRP	64
Statistique Canada : Repenser les projets intrusifs de collecte de données en tenant compte du respect de la vie privée	32	Tableaux relatifs à la LPRPDE	75
Autres enquêtes majeures	36	Annexe 3 : Processus d'enquête	80
Mise à jour sur les déclarations d'atteintes à la vie privée	41	Processus d'enquête en vertu de la LPRP	80
Conseils aux institutions fédérales	42	Processus d'enquête en vertu de la LPRPDE	82
La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) – Rétrospective de l'exercice	46	Annexe 4 : Lois essentiellement similaires	84
Mises à jour et tendances en matière de fonctionnement	47	Annexe 5 : Rapport de la commissaire spéciale à la protection de la vie privée	85
Facebook refuse de corriger les lacunes constatées en matière de protection de la vie privée	47		
Lacunes en matière de sécurité menant à une atteinte massive chez Equifax	49		
Autres enquêtes majeures	50		
Loi canadienne anti-pourriel (LCAP)	52		
Mise à jour sur les déclarations d'atteintes	53		



Message du commissaire

À l'instar de mes prédécesseurs, je réclame depuis plusieurs années une réforme fondamentale des lois sur la protection des renseignements personnels dans les secteurs privé et public au Canada. Au cours de l'exercice écoulé, le gouvernement a enfin reconnu que le moment était venu de procéder à une réforme législative. Les membres du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) – tous partis politiques confondus – s'entendent aussi sur ce point. Même les géants de la haute technologie proclament que l'ère de l'autoréglementation est révolue. La question n'est plus de savoir si l'on doit ou non moderniser les lois sur la protection des renseignements personnels. Il s'agit maintenant de déterminer comment procéder.

La protection de la vie privée est un concept contextuel parfois difficile à définir avec précision. Elle n'en demeure pas moins un droit fondamental et une valeur de base dans la société canadienne. Comme nous l'avons vu récemment dans le scandale Cambridge Analytica, la vie privée est une condition préalable à l'exercice d'autres droits fondamentaux, notamment la liberté, l'égalité et la démocratie. Le point de départ devrait consister à faire en sorte que les nouvelles lois sur la protection des renseignements personnels soient fondées sur les droits.

Les technologies axées sur les données présentent incontestablement des avantages pour les individus. Elles rendent notre vie plus agréable et offrent

d'innombrables services pratiques. De façon plus fondamentale, elles peuvent constituer de puissants outils pour l'épanouissement personnel. Ces technologies ouvrent aussi la voie à d'énormes possibilités pour l'amélioration des soins de santé, de l'environnement et de la croissance économique. En revanche, elles créent de nouveaux risques. Pour le meilleur ou pour le pire, ce sont des technologies perturbatrices.

Tim Cook d'Apple a dénoncé l'an dernier la formation d'un « complexe industriel de données personnelles » en soulignant que « nos données personnelles – de notre vie quotidienne jusqu'à notre plus grande intimité – sont aujourd'hui utilisées contre nous avec une efficacité toute militaire ». À ses yeux, « c'est de la surveillance ». La chercheuse américaine Shoshana Zuboff décrit le nouveau modèle économique en termes similaires, le qualifiant de « capitalisme de la surveillance ». Et Yoshua Bengio, spécialiste canadien de l'intelligence artificielle, estime que la seule manière de rétablir l'équilibre, c'est que l'individu ne reste pas seul face à l'entreprise; selon lui, c'est le rôle des gouvernements de protéger les individus.

Les nouvelles lois sur la protection des renseignements personnels devraient permettre une innovation responsable, mais je partage complètement l'idée que l'on ne devrait pas laisser les individus seuls face à l'entreprise. La protection de la vie privée est souvent considérée à travers le prisme des politiques de confidentialité des sites Web menant à une forme imparfaite du consentement. Il s'agit toutefois d'un point de vue réducteur qui défavorise nettement les individus

lorsqu'ils sont confrontés à des organisations ayant infiniment plus de connaissances et de pouvoir.

Les règles techniques – par exemple celles régissant le consentement, l'accès et la transparence – constituent des mécanismes importants pour la protection des renseignements personnels, mais elles ne définissent pas le droit à la vie privée proprement dit. La législation devrait définir la protection de la vie privée dans son sens le plus large et le plus véritable, par exemple en la décrivant comme l'absence d'une surveillance injustifiée. Les Canadiens veulent profiter des avantages des technologies numériques, mais en toute sécurité. La législation devrait reconnaître et protéger la liberté de vivre et de s'épanouir de façon autonome, à l'abri du regard scrutateur d'un État de surveillance ou d'entreprises commerciales. Les Canadiens devraient être en mesure de participer activement mais de façon sécuritaire à la vie quotidienne telle qu'on la connaît dans une société numérique moderne.

On s'entend généralement sur la nécessité de la réforme législative. Toutefois, le vocabulaire utilisé par les représentants de l'industrie et du gouvernement continue de trahir l'importance qu'ils accordent à l'atteinte d'un juste équilibre entre, d'une part, le droit à la vie privée et, d'autre part, les intérêts économiques, la sécurité et d'autres objectifs importants. Ils laissent entendre que la protection de la vie privée et des objectifs tels que l'innovation sont engagés dans ce que certains appellent « un jeu à somme nulle ».

Nous devons rejeter l'idée que les lois fondées sur le respect des droits nuisent à la croissance économique ou à d'autres objectifs sociétaux importants. Les droits fondamentaux ne freinent ni l'innovation ni la prestation des services gouvernementaux à l'ère numérique. En réalité, une loi fondée sur les droits favoriserait une innovation responsable en renforçant la confiance dans les activités gouvernementales et commerciales.

On peut affirmer sans crainte d'exagérer que la numérisation de tant d'aspects de nos vies est en train de transformer l'humanité. Si nous ne faisons pas attention, elle prendra une forme qui ne correspond pas à nos valeurs ni à nos droits les plus fondamentaux. Par conséquent, on ne devrait pas autoriser les utilisations de la technologie qui sont incompatibles avec ces valeurs et ces droits. Le marché a prouvé à maintes

reprises qu'il est créatif. Il trouvera des moyens rentables d'offrir des produits et des services qui répondent à des besoins véritables, tout en respectant un cadre législatif renouvelé qui respecte ces droits et ces valeurs. Il devrait en aller de même des gouvernements démocratiques soumis à la règle de droit.



On peut affirmer sans crainte d'exagérer que la numérisation de tant d'aspects de nos vies est en train de transformer l'humanité. Si nous ne faisons pas attention, elle prendra une forme qui ne correspond pas à nos valeurs ni à nos droits les plus fondamentaux.

Nous avons consacré un chapitre du présent rapport annuel à l'exploration de plusieurs enjeux concernant la réforme législative, notamment la façon de mettre en œuvre de façon efficace une approche fondée sur les droits pour protéger la vie privée des Canadiens. Permettez-moi de souligner ici quelques-uns des éléments les plus importants de cette approche.

Premièrement, la loi devrait pouvoir résister au passage du temps, c'est-à-dire qu'elle devrait demeurer pertinente malgré les avancées technologiques. Ces avancées se produisent à un rythme exponentiel; il est tout simplement impossible de modifier la loi à la même vitesse. Cet argument en faveur d'une législation fondée sur les principes, qu'invoquent l'industrie et le gouvernement, justifie également une législation qui définit la protection de la vie privée dans son sens le plus large et le plus véritable. Les mesures de protection techniques, par exemple faire reposer la validité du consentement sur certains éléments d'information, s'avèrent souvent inefficaces, car elles sont la plupart du temps dépassées par les avancées technologiques. Cependant, les valeurs sous-jacentes au droit à la vie privée ne changeront probablement pas beaucoup au fil du temps. En définissant la vie privée de manière à lui donner tout son sens, conforme aux valeurs qui la sous-tendent, on s'assurerait qu'elle demeure protégée peu importe les changements technologiques.

Deuxièmement, la loi applicable au secteur privé devrait véritablement et résolument mettre fin à l'autoréglementation. Cela signifie, en partie, qu'une autorité publique devrait être habilitée à établir des règles subsidiaires contraignantes, concrétisant ainsi les principes dans des contextes particuliers. De cette façon, les individus et les organisations commerciales et gouvernementales connaîtraient leurs droits et obligations d'une manière plus certaine. L'autorité publique en question pourrait être le Commissariat, un ministère ou une autre entité de l'État. Les codes de l'industrie et les règles d'éthique ont leur place, ils peuvent offrir une plus grande transparence et une plus grande uniformité dans l'application de la loi, mais ils ne sont pas juridiquement contraignants ni exécutoires et ils ne peuvent remplacer les règles adoptées par l'État dans l'intérêt public. Sans règles subsidiaires contraignantes, les organisations ont un pouvoir discrétionnaire excessif leur permettant d'appliquer les principes comme bon leur semble, ce qui revient en quelque sorte à vider ces principes de leur substance et à établir une forme d'autoréglementation. Or, nous avons pu observer au cours des dernières années les risques et les limites de cette approche.

Ce qu'il faut, c'est une loi qui assure une responsabilité démontrable, c'est-à-dire une responsabilité que l'entreprise doit démontrer à l'organisme de réglementation, soit un tiers indépendant.

Une autre forme d'autoréglementation subsisterait si l'on conservait tel quel le principe de responsabilité compris dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) ou si l'on en augmentait l'importance. Les milieux d'affaires prônent la responsabilité en tant qu'élément important de la protection de la vie privée. L'industrie fait valoir que nous devrions lui donner encore plus d'importance en soutenant, à juste titre, que le consentement est de plus en plus inefficace pour protéger la vie privée. Je reconnais l'importance de la responsabilité. Toutefois, comme nous l'avons si clairement constaté dans les

dossiers de Facebook et d'Equifax ainsi que dans d'autres cas, ce principe dans sa forme actuelle est insuffisant pour protéger les Canadiens contre les pratiques d'entreprises qui prétendent agir de manière responsable alors que ce n'est manifestement pas le cas.

Ce qu'il faut, c'est une loi qui assure une responsabilité démontrable, c'est-à-dire une responsabilité que l'entreprise doit démontrer à l'organisme de réglementation, soit un tiers indépendant. Dans un monde où les modèles d'affaires sont opaques et où les flux d'information sont de plus en plus complexes, les individus ne sont guère susceptibles de déposer une plainte s'ils ne sont pas au courant des pratiques qui peuvent leur porter préjudice. C'est pourquoi il est si important de donner à l'organisme de réglementation le pouvoir d'inspecter de son propre chef les pratiques des organisations. Lorsque l'obtention du consentement est impraticable et que les organisations sont censées pallier le manque en se montrant responsables, il faut obliger ces dernières à faire la preuve de leur responsabilité sur demande.

La responsabilité démontrable fait aussi partie de la solution pour protéger les Canadiens dans le contexte des flux de données transfrontières. Je reconnais que ces flux sont assujettis aux accords commerciaux internationaux et qu'ils procurent des avantages considérables aux individus et aux organisations, mais je suis aussi convaincu que le gouvernement a l'obligation de protéger la vie privée de ses citoyens en adoptant des lois efficaces en la matière. Notre enquête sur Equifax a démontré que le principe de responsabilité énoncé dans la LPRPDE ne protège pas toujours efficacement les Canadiens dans le cadre des transferts internationaux. Il faut renforcer la loi, à tout le moins en adoptant le principe de responsabilité démontrable, voire par d'autres moyens, par exemple en s'inspirant du régime européen de clauses contractuelles types.

Troisièmement, l'adoption des principes de nécessité et de proportionnalité dans la loi applicable au secteur public constitue un autre élément clé de l'approche fondée sur les droits en matière de réforme législative. Au moyen des technologies numériques, le gouvernement peut beaucoup plus facilement recueillir, communiquer, utiliser et stocker les renseignements personnels des individus. Le passage des documents papier au

format numérique a, en fait, créé une dynamique de collecte excessive. Notre enquête sur Statistique Canada a démontré qu'une collecte excessive de renseignements personnels ne répondant pas aux critères de nécessité et de proportionnalité peut porter une grave atteinte à la vie privée. Il serait plus conforme à la nature quasi constitutionnelle de la *Loi sur les renseignements personnels* (LPRP) que la collecte des renseignements personnels par le gouvernement se limite explicitement à ceux qui sont manifestement nécessaires à un programme ou à une activité, et qu'elle soit proportionnelle au risque d'atteinte à la vie privée. De nombreuses économies membres de l'Organisation de coopération et de développement économiques (OCDE), ainsi que la plupart des provinces et des territoires du Canada, ont adopté la norme de la nécessité en matière de collecte de renseignements. La législation fédérale devrait faire de même afin de refléter la réalité moderne et les attentes actuelles.

Quatrième et dernier point, la loi devrait prévoir des mécanismes d'application garantissant aux individus un recours rapide et efficace pour la protection de leur droit à la vie privée. Ces mécanismes devraient aussi inciter les institutions fédérales et les organisations commerciales à se conformer de façon générale à la loi en tout temps.

Malheureusement, les lois canadiennes accusent un énorme retard par rapport à celles des partenaires commerciaux du Canada en ce qui concerne l'application des lois sur la protection des renseignements personnels. Par ailleurs, la plupart des Canadiens estiment que les organisations ne respectent pas leur droit à la vie privée. Il s'agit là d'un blâme accablant et, à mon avis, d'une situation intolérable dans un pays régi par la primauté du droit. Cet état de choses ne favorise certes pas la confiance des consommateurs, qui constitue l'un des objectifs déclarés du gouvernement.

La Charte numérique du gouvernement mentionne qu'il faudrait accorder au Commissariat un pouvoir « limité » de rendre des ordonnances. En outre, toujours selon la Charte, je devrais, après avoir mené ma propre enquête, convaincre le procureur général de faire enquête de nouveau et, à terme, de porter l'affaire devant la cour avant que des amendes ne puissent être imposées aux contrevenants. Par comparaison, mes homologues européens et américains, entre autres, peuvent ordonner

directement aux entreprises de se conformer à la loi et leur imposer des amendes assez lourdes, bien entendu sous réserve d'un contrôle judiciaire. À mon avis, la proposition du gouvernement est complètement inefficace puisque les individus ne pourraient jouir de leur droit à la vie privée que plusieurs années après avoir déposé une plainte. Justice différée, justice refusée.

Un véritable pouvoir de rendre des ordonnances et d'imposer des amendes aurait un effet sur la dynamique de nos échanges avec les entreprises dans le cadre d'enquêtes, ce qui mènerait à des règlements plus rapides pour le compte des Canadiens. À l'heure actuelle, comme nous l'avons constaté au cours de l'enquête visant Facebook, une entreprise que l'on estime avoir contrevenu à la loi peut tout simplement faire fi de nos recommandations et s'arroger un sursis jusqu'à ce que les tribunaux en soient venus aux mêmes conclusions que le Commissariat. Le projet de Charte numérique du gouvernement prévoit l'étape additionnelle d'un examen par le procureur général.

Tant le cadre existant que la proposition du gouvernement sont d'excellents incitatifs pour les entreprises à ne pas prendre la vie privée au sérieux, à ne changer leurs pratiques que si elles sont contraintes à le faire au terme d'années de procédures judiciaires, se contentant généralement de faire des affaires sans se préoccuper outre mesure de la conformité avec les lois sur la protection des renseignements personnels.

Selon mes homologues provinciaux et étrangers qui ont déjà été dotés de pouvoirs de rendre des ordonnances et d'imposer des sanctions pécuniaires, les entreprises semblent beaucoup plus enclines à collaborer avec eux depuis qu'ils ont été dotés de ces outils. Dans les cas où l'autorité de réglementation conclut qu'il y a eu manquement à la loi, les entreprises corrigent plus facilement le tir sans délais indus.

En fin de compte, les mécanismes d'application de la loi devraient offrir aux individus des recours rapides et efficaces et assurer une conformité générale et constante des organisations et des institutions. C'est seulement de cette manière que la confiance envers les pratiques numériques des entreprises et du gouvernement atteindra le niveau que nous souhaitons tous.

La protection de la vie privée en chiffres

1 420

Plaintes en vertu
de la LPRP acceptées

380

Plaintes en vertu de
la LPRPDE acceptées

315

Déclarations d'atteinte
à la sécurité des données en
vertu de la LPRPDE examinées

433

Plaintes en vertu de la LPRP
fermées par règlement rapide

178

Plaintes en vertu de la LPRPDE
fermées par règlement rapide

21

Activités de liaison des services-
conseil avec le secteur privé

933

Plaintes en vertu de la LPRP
fermées à l'issue d'une
enquête officielle

104

Plaintes en vertu de la LPRPDE
fermées à l'issue d'une
enquête officielle

23

Lois, projets de loi et études
parlementaires examinées sous l'angle
de leurs répercussions sur la vie privée

155

Déclarations d'atteinte
à la sécurité des données
en vertu de la LPRP examinées

87

Avis donnés à des organisations
du secteur public à la suite de
l'examen d'une EFVP ou d'une
consultation à cet égard

14

Mémoires officiels présentés au
Parlement sur des questions
touchant les secteurs privé et public

56

Annonces et
communiqués diffusés

76

Évaluations des facteurs
relatifs à la vie privée
(EFVP) reçues

383

Communications de
renseignements dans l'intérêt
public par les institutions fédérales

10 200

Demandes d'information

1 098

Gazouillis envoyés

48

Activités de liaison des
services-conseils avec
le secteur public

16

Comparutions devant des comités
parlementaires sur des questions
touchant les secteurs privé et public

75

Allocutions et présentations

15 301

Abonnés sur Twitter

2 808 560

Consultations du site Web

208 282

Consultations du blogue

45 598

Publications diffusées

Conseils au Parlement





Réforme des lois sur la protection des renseignements personnels : une voie vers le respect des droits et le rétablissement de la confiance envers le gouvernement et l'économie numérique

Introduction

Dans ses trois derniers rapports annuels, le Commissariat à la protection de la vie privée du Canada a présenté au Parlement une analyse détaillée des raisons pour lesquelles les Canadiens ont besoin de lois fédérales sur la protection des renseignements personnels plus strictes et plus contraignantes. Les technologies de l'information utilisées au sein de l'économie et de l'administration publique évoluent rapidement, d'où la nécessité d'une réforme législative. Les avancées numériques à nos portes reposent de plus en plus sur la collecte et la communication d'une quantité massive de renseignements, la prise de décisions automatisée et le profilage. Les répercussions sur la vie privée et, par ricochet, les risques d'atteinte aux droits et libertés fondamentaux sont énormes.

Récemment, le gouvernement du Canada a lui aussi reconnu que le moment était venu d'améliorer nos lois sur la protection des renseignements personnels. En réponse au rapport sur l'examen de la LPRP publié en décembre 2016 par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), le gouvernement s'est engagé à lancer son propre examen en vue de moderniser cette loi. Le Comité a également publié en février 2018 un rapport sur l'examen de la LPRPDE. Le gouvernement était d'accord avec le Comité sur la nécessité de modifier le régime canadien de protection de la vie privée pour « veiller à ce que les règles d'utilisation des renseignements personnels dans un contexte commercial soient claires et applicables et permettent d'assurer le niveau de protection de la vie privée auquel les Canadiens s'attendent ».

Le Comité ETHI a récemment publié un rapport intitulé *Démocratie menacée : Risques et solutions à l'ère de la désinformation et du monopole des données*. Il y formule à l'intention du gouvernement plusieurs recommandations visant à s'attaquer à l'autoréglementation des monopoles de plateforme et aux vulnérabilités connexes de nos processus démocratique et électoral attribuables à l'acquisition et au traitement inappropriés de renseignements personnels. Dans sa réponse à ce rapport, le gouvernement a convenu une fois encore qu'il faut moderniser le régime canadien de protection de la vie privée en imposant des règles claires et applicables pour protéger la vie privée des Canadiens.

Peu après la réponse du gouvernement à ce rapport du Comité ETHI, Innovation, Sciences et Développement économique Canada (ISDE) a publié un projet de modernisation de la LPRPDE. Pour sa part, le ministère de la Justice a publié un plan d'action pour mobiliser les intervenants en vue de moderniser la LPRP.

Pour en savoir davantage

ETHI, *Protéger la vie privée des Canadiens : Examen de la Loi sur la protection des renseignements personnels*, décembre 2016)

Réponse du gouvernement du Canada à Protéger la vie privée des Canadiens : Examen de la Loi sur la protection des renseignements personnels, avril 2017

ETHI, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, février 2018

Réponse du gouvernement du Canada à Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques, juin 2018

ETHI, *Démocratie menacée : Risques et solutions à l'ère de la désinformation et du monopole des données*, décembre 2018

Réponse du gouvernement du Canada à *Démocratie menacée : Risques et solutions à l'ère de la désinformation et du monopole des données*, janvier 2019

ISDE, *Renforcer la protection de la vie privée dans l'ère numérique*, mai 2019

Ministère de la Justice, *Modernisation de la Loi sur la protection des renseignements personnels du Canada*, août 2019

Ailleurs dans le monde, les lois sur la protection des renseignements personnels ont été renforcées dans plusieurs territoires de compétence afin de relever les défis du numérique. Il est manifeste que la réforme des lois sur la protection des renseignements personnels prend de l'ampleur à l'échelle planétaire. Partout dans le monde, les gouvernements et les législateurs ont constaté les lacunes des modèles d'autoréglementation et les menaces que ces modèles font peser dans une économie numérique mondialisée. Nous espérons que le Canada est prêt à prendre des mesures fermes et décisives pour moderniser nos lois sur la protection des renseignements personnels, afin de mieux protéger les droits des Canadiens lorsqu'ils interagissent avec les entreprises et le gouvernement dans ce monde de plus en plus numérique, où les renseignements personnels sont devenus une importante monnaie d'échange.

Soyons clairs : nous reconnaissons que le numérique permet d'offrir de meilleurs services, qu'il s'agisse des services du gouvernement aux citoyens ou encore des services d'entreprises aux consommateurs.

Le numérique a permis de trouver des solutions créatives qui ont permis d'améliorer la manière dont le gouvernement et les entreprises fonctionnent, et la manière dont les gens socialisent et communiquent ensemble. On crée des services numériques qui profitent à la société de toutes sortes de façons, depuis les nouveaux appareils de santé jusqu'aux technologies visant à protéger l'environnement. Une telle innovation est vitale pour la croissance économique du Canada. Un cadre législatif solide qui ferait du Canada un chef de file en matière de protection de la vie privée ne ferait que renforcer notre position concurrentielle.

D'après nous, les lois fédérales sur la protection des renseignements personnels au Canada devraient demeurer neutres sur le plan technologique et fondées sur des principes. Ces deux caractéristiques permettront à ces lois d'établir des règles uniformes dans l'ensemble des secteurs de l'industrie et de résister au passage du temps; les lois garderaient ainsi leur pertinence malgré le rythme exponentiel des avancées technologiques. Certes, le développement rapide de nouvelles technologies nécessitera à l'occasion des modifications législatives; il faudra examiner nos lois périodiquement, potentiellement tous les cinq ans environ. Toutefois, du fait qu'elles seront fondées sur des principes, elles devraient demeurer pertinentes sans que l'on doive constamment les réviser pour maintenir le rythme.

Par ailleurs, nous estimons que les Canadiens méritent aussi des lois fédérales en la matière qui soient fondées sur les droits des individus. L'intégration d'un cadre fondé sur les droits permettrait d'appuyer une innovation responsable et de susciter la confiance envers le gouvernement. Cela permettrait aux gens de participer pleinement et en toute confiance à l'économie numérique. Nous sommes convaincus que les organisations des secteurs privé et public pourront continuer d'innover et de prospérer dans un environnement qui, d'une part, appuie et favorise l'innovation et qui, d'autre part, reconnaît et protège le droit à la vie privée des personnes. En fait, en mettant davantage l'accent sur le droit à la vie privée, les pratiques responsables et la transparence, on pourrait aider le milieu des affaires et le secteur public à demeurer concurrentiels et pertinents à l'échelle nationale et internationale, compte tenu de l'évolution de la situation sur ce plan dans le monde.

Dans le présent chapitre, nous indiquons ce que nous entendons par une approche fondée sur les droits pour protéger la vie privée des Canadiens. Nous expliquons des options possibles pour adapter aux réalités du 21^e siècle les lois fédérales sur la protection des renseignements personnels. En conclusion, nous procédons à une analyse générale de plusieurs éléments clés que nous jugeons essentiels pour la réforme des lois sur la protection des renseignements personnels au Canada.

Reconnaissance du droit à la vie privée en tant que droit de la personne

De par sa nature, la vie privée est une valeur très chère aux Canadiens et profondément ancrée dans une tradition des droits de la personne.

Dès 1948, le Canada a reconnu les droits de la personne et conclu des accords internationaux qui ont fait date dans le domaine. Ces accords garantissaient résolument le droit à la vie privée en tant que droit fondamental à la dignité et à l'intégrité humaines, ainsi qu'à l'honneur et à la réputation d'une personne, et assuraient une protection contre l'ingérence arbitraire dans la vie ou les communications privées d'une personne. En 1968, le Comité permanent de la justice et des questions juridiques a demandé pour la première fois au gouvernement de créer une législation sur la protection

des renseignements personnels. Par suite de discussions tenues à la réunion de l'Association du Barreau canadien de cette année-là, le ministère de la Justice du Canada a commencé à rédiger l'ébauche d'un projet de loi sur la protection des renseignements personnels. Ces efforts ont abouti aux premières mesures législatives adoptées au Canada pour protéger les renseignements personnels contre les actions du secteur public fédéral. Ces mesures de protection, adoptées en 1977 dans les dispositions antidiscriminatoires prévues à la partie IV de la *Loi canadienne sur les droits de la personne*, ont été suivies en 1983 par la promulgation de la *Loi sur la protection des renseignements personnels*.

Pour en savoir davantage

Projet de loi S-21, Loi visant à garantir le droit des individus au respect de leur vie privée, 2001

Cour suprême du Canada, *R. c. Spencer*, 2014

Cour suprême du Canada, *R. c. Jones*, 2017

Cour suprême du Canada, *R. c. Jones*, 2019

41^e Conférence internationale des commissaires à la protection des données et de la vie privée, *Résolution internationale sur la protection de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits fondamentaux*, 2019

On a aussi observé au palier fédéral des tentatives de renforcer et d'officialiser davantage le droit à la vie privée. En 2000, la sénatrice Sheila Finestone a déposé le *Projet de loi S-21, Loi visant à garantir le droit des individus au respect de leur vie privée* (« la Charte Finestone ») au Sénat du Canada. Ce projet de loi visait à situer le droit à la vie privée dans le cadre plus vaste des droits de la personne et, en le situant dans cette perspective, à faciliter son interprétation dans un sens large. Aux termes de la Charte Finestone, le droit à la vie privée comporte le droit au respect de son intimité physique, le droit d'être libre de toute surveillance, le droit d'être à l'abri du contrôle et de l'interception de ses communications privées et le droit d'être à l'abri de la collecte, de l'utilisation et de la communication de ses renseignements personnels.

Depuis l'époque de ce projet de charte, la Cour suprême du Canada a approfondi sa compréhension de la vie privée et l'a appliquée dans toute une gamme de contextes. Mentionnons entre autres, sans s'y limiter, la liste des activités que la Charte Finestone visait à protéger. Dans l'arrêt *R. c. Spencer*, la Cour suprême du Canada a reconnu que la protection de la vie privée comprend ce qui suit : la notion de confidentialité; le contrôle, l'accès et l'utilisation de renseignements personnels; et l'anonymat. Plus récemment, dans l'arrêt *R. c. Jarvis*, la Cour suprême du Canada a confirmé que la protection de la vie privée n'est pas un concept absolu et que le fait de se trouver dans un lieu public ou semi-public n'entraîne pas automatiquement une renonciation à toute attente de protection en la matière au chapitre de l'observation ou de l'enregistrement.

La Cour suprême a aussi reconnu à maintes reprises que la protection de la vie privée est nécessaire à l'exercice d'autres droits de la personne protégés par la *Charte canadienne des droits et libertés* et a confirmé le statut quasi constitutionnel des lois fédérales et provinciales sur la protection des renseignements personnels. Dans l'arrêt *R. c. Jones*, la Cour suprême du Canada a également reconnu que la protection de la vie privée est essentielle pour assurer la dignité, l'autonomie et la croissance personnelle d'une personne et, par conséquent, que la protection de la vie privée des individus est une condition préalable essentielle à l'épanouissement d'une démocratie libre et en santé.

Malgré cette reconnaissance traditionnelle de la protection de la vie privée en tant que droit de la personne fondamental nécessaire à l'exercice d'autres droits, nos lois actuelles sur la protection des renseignements personnels sont, de fait, des instruments qui protègent principalement les données, plutôt que des lois qui protègent et favorisent l'exercice d'un large éventail de droits. La protection de la vie privée ne se limite pas au consentement, à l'accès et à la transparence. Ces mécanismes sont importants, mais ils ne définissent pas le droit proprement dit et ne reconnaissent pas son statut quasi constitutionnel. Il faut remanier nos lois de manière à reconnaître que le droit à la vie privée n'est rien de moins qu'une condition préalable à la liberté : la liberté de vivre et de s'épanouir de façon autonome, à l'abri de la surveillance de l'État ou d'entreprises commerciales, tout en

participant pleinement aux activités courantes d'une société moderne. Cette idée trouve un écho parmi la collectivité des commissaires, comme on le constate par l'adoption de la résolution sur la vie privée comme droit fondamental et condition préalable à l'exercice d'autres droits dans le cadre de la 41^e Conférence internationale des commissaires à la protection des données et de la vie privée en octobre 2019.

Les choses ont beaucoup changé depuis 2000, année où la sénatrice Finestone a déposé sa charte. Mais, de toute évidence, le droit à la vie privée mérite encore aujourd'hui d'être protégé en vertu de la loi. Des lois sur la protection des renseignements personnels modernisées devraient reconnaître de prime abord la portée réelle du droit à la vie privée et son statut quasi constitutionnel. De concert avec leur fondement sur des principes et leur neutralité du point de vue technologique, nos lois résisteraient à l'épreuve du temps, seraient compatibles avec celles d'autres territoires de compétence et refléteraient les valeurs canadiennes.

Une approche fondée sur les droits pour protéger la vie privée des Canadiens

Comme nous l'avons mentionné, les lois fédérales actuelles sur la protection des renseignements personnels au Canada ont une portée étroite sur la protection des données. La LPRPDE et la LPRP établissent un ensemble de règles qui encadrent la façon dont les organisations et les institutions fédérales doivent traiter les renseignements personnels des individus. Quoique ces deux lois garantissent le droit d'accès des individus aux renseignements personnels qui les concernent, et leur confèrent aussi le droit de demander la correction de ces renseignements et de déposer une plainte auprès du Commissariat, aucune ne reconnaît officiellement le droit à la vie privée comme un droit en soi. La protection de la vie privée est plus large que la protection des données, bien que la seconde contribue à la première. Pour que nos lois sur la protection des données protègent plus efficacement la vie privée dans un sens plus large, ce but doit être exprimé plus explicitement dans la formulation des lois en matière de protection des renseignements personnels.

De nombreux instruments internationaux récemment adoptés ou mis à jour comprennent des mesures en ce sens, bien qu'il subsiste un manque d'harmonisation. Par exemple, l'Union européenne a adopté dans le *Règlement général sur la protection des données* (RGPD) une approche fondée sur les droits de la personne pour la protection de la vie privée. Dans les 173 points de son préambule, le RGPD renvoie à maintes reprises aux droits fondamentaux des personnes à l'égard du traitement des données. Par exemple, selon le point 2, « les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux ». Comme l'indique Teresa Scassa dans un texte intitulé « A Rights-Based Approach to Data Protection in Canada » (2019, en anglais seulement), l'intégration des droits de la personne dans le RGPD présente l'avantage de faciliter la conciliation des droits plus récents et plus modernes que dans une conception étroite de la protection des données. Elle fait remarquer notamment que le droit à l'oubli ne se limite pas au droit d'un individu d'exercer un contrôle sur ses renseignements personnels. Il est aussi lié au droit de s'épanouir en tant que personne, ce qui permet de faire des expériences, de commettre des erreurs et de recommencer à neuf dans un environnement en ligne. Cette démarche va donc plus loin que la simple protection des données et suppose un droit fondamental à la vie privée.

Pour en savoir davantage

[Règlement général sur la protection des données de l'Union européenne](#)

[Aperçu des lois sur la protection des renseignements personnels au Canada](#)

[Lois provinciales réputées essentiellement similaires à la LPRPDE](#)

Rapport de conclusions : [Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc.](#)

Pour être clairs, nous n'avancions pas que le droit canadien ne prévoit pas d'autres types de mesures de protection de la vie privée ailleurs que dans les lois de protection des données. Plusieurs lois canadiennes protègent le droit à la vie privée, et divers ordres de gouvernement et diverses instances judiciaires se chargent de leur application. Comme nous y avons fait allusion précédemment, les tribunaux se sont appuyés sur l'article 7 (droit à la vie, à la liberté et à la sécurité de sa personne) et l'article 8 (droit à la protection contre les fouilles, les perquisitions ou les saisies abusives) de la *Charte canadienne des droits et libertés* pour protéger les individus contre les atteintes inacceptables à leur vie privée par l'État.

Tout comme les droits de la personne en général, le droit à la vie privée n'est pas exclusivement de compétence fédérale au Canada. Des lois provinciales s'appliquent au traitement des données personnelles par les gouvernements provinciaux et plusieurs lois provinciales sont considérées comme essentiellement similaires à la LPRPDE. À bien des égards, ces lois offrent de meilleures mesures de protection que les lois fédérales en la matière.

Dans cet environnement complexe où des mesures de protection de la vie privée propres au contexte sont réparties entre différentes administrations publiques, avec en toile de fond une croissance accélérée de l'économie axée sur les données, il serait utile que le gouvernement fédéral reconnaisse plus complètement le droit à la vie privée conféré aux individus. Il préciserait ainsi au bénéfice des organisations publiques et privées les obligations leur incombant de protéger la vie privée des individus, tout en apportant à ces derniers une plus grande certitude concernant leur capacité d'exercer leurs droits à cet égard et de les faire respecter.

Nous proposons de modifier nos deux lois fédérales sur la protection des renseignements personnels de manière à leur donner une assise fondée sur les droits, reconnaissant le droit à la vie privée dans toute sa portée et son ampleur, et assurant une orientation sur la façon d'interpréter leurs autres dispositions. Cette orientation pourrait prendre une forme similaire au texte proposé à la fin du présent chapitre.

Par ailleurs, nous estimons qu'une loi fondée sur les droits devrait comprendre les éléments clés suivants :

1) Définir le droit à la vie privée dans son sens

le plus large, ce qui signifie établir explicitement dans la loi que l'un des objectifs fondamentaux de la législation devrait être de protéger le droit à la vie privée en tant que droit de la personne en soi, de même qu'en tant qu'élément essentiel à la réalisation et à la protection d'autres droits de la personne. Au sens large, la vie privée pourrait, comme dans la Charte Finestone, se définir en outre comme « l'absence de surveillance injustifiée », ce dernier mot confirmant que la vie privée n'est pas un droit absolu. La définition devrait aussi refléter la riche jurisprudence en la matière, notamment celle de la Cour suprême du Canada.

2) Reconnaître la nature quasi constitutionnelle des lois sur la protection des renseignements personnels, ce qui signifie de confirmer que

la vie privée est protégée comme l'a établi la Cour suprême du Canada dans ses décisions, où elle a reconnu le rôle fondamental de la vie privée dans la préservation d'une société libre et démocratique.

3) Rédiger la loi de la manière habituelle, avec des obligations et des droits clairement énoncés dans le texte de la loi, plutôt que d'adopter le

modèle actuel, qui comprend un document rédigé comme un code de conduite de l'industrie, et qui prévoit certaines obligations mais aussi plusieurs recommandations, exemples et pratiques exemplaires qui ne constituent pas des droits juridiquement protégés pour les individus. Les tribunaux ont reconnu que la rédaction non juridique de la LPRPDE présentait des enjeux, la rendant difficilement accessible et ne prévoyant pas ou très peu d'orientation à ceux chargés de son interprétation.

4) Assurer une application efficace de la loi, c'est-à-dire adopter des mécanismes qui se traduiraient par des recours rapides et efficaces pour les individus, et par une conformité générale et continue pour les organisations et les institutions. En l'absence d'une application efficace de la loi, on vide les droits de leur substance, et la confiance se dissipe.

Parmi les améliorations requises, mentionnons celle de donner au commissaire à la protection de

la vie privée du Canada les moyens nécessaires pour effectuer des inspections proactives, de rendre des ordonnances exécutoires et d'imposer des sanctions en cas de non-conformité à la loi. Les inspections proactives sont abordées plus loin dans le présent chapitre, dans la section sur la responsabilité démontrable. Ces inspections sont nécessaires pour assurer le respect continu de la loi, contrairement au système actuel où les violations doivent d'abord être cernées (ce qui n'est pas une tâche facile en cette ère numérique), puis faire l'objet d'une enquête et, finalement, être corrigées volontairement par une organisation, pour que le respect de la loi puisse enfin être rétabli. Les inspections proactives, combinées aux ordonnances et aux amendes, encouragent la conformité continue et, par conséquent, permettent d'améliorer grandement la confiance des consommateurs.

Dans d'autres territoires de compétence au Canada et à l'étranger, les organismes de réglementation de la protection de la vie privée ou des données ont l'autorité nécessaire pour rendre des ordonnances exécutoires et imposer des sanctions pécuniaires, sous réserve d'un contrôle judiciaire. Donner ces pouvoirs à une autorité de premier niveau plutôt que d'obliger les individus à attendre qu'un tribunal, plusieurs années après une violation présumée, confirme le bien-fondé d'une plainte, est un moyen beaucoup plus efficace d'assurer une jouissance plus rapide des droits. Encore une fois, c'est le choix législatif qu'ont fait plusieurs provinces canadiennes, ainsi que nombre de partenaires commerciaux du Canada, dont les États-Unis et l'Union européenne. Le droit des Canadiens à la vie privée devrait être protégé de manière aussi efficace que s'ils vivaient dans d'autres territoires de compétence.

Bien que des pouvoirs accrus pour le Commissariat fassent partie de la solution, ils ne sont pas les seuls du point de vue de l'application de la loi. Avec des ressources limitées et une multitude de rôles et de responsabilités, le Commissariat ne peut enquêter sur toutes les infractions à la loi. Dans un modèle fondé sur les droits, il est important que les individus aient un droit de recours indépendant devant les tribunaux pour demander réparation en cas de non-respect de leurs droits.

Des événements survenus au cours de l'année ont mis en évidence, plus que jamais auparavant, l'urgence de moderniser le mode de protection du droit à la vie privée au Canada. Pour ne citer qu'un exemple, soulignons que notre enquête sur Facebook a démontré que l'entreprise avait commis des infractions graves aux lois canadiennes sur la protection des renseignements personnels. Cette enquête faisait suite à des révélations selon lesquelles Facebook avait communiqué les renseignements personnels de certains utilisateurs à une application tierce, qui avait ensuite utilisé cette information pour leur envoyer des messages politiques ciblés. En réponse, l'entreprise a réfuté nos conclusions d'enquête. Elle a refusé de régler les graves problèmes que nous avons relevés et de reconnaître qu'elle avait contrevenu à la loi.

Cette situation fait ressortir de graves lacunes dans notre cadre actuel de protection de la vie privée. Il est intenable qu'une entreprise comme Facebook rejette les conclusions d'enquête du Commissariat et qu'elle s'arroge le pouvoir de décider par elle-même à quelles obligations légales elle se conformera ou non. Le Canada a besoin de lois sur la protection des renseignements modernisées assurant une application et des recours efficaces et considérant la protection de la vie privée dans tout le spectre des droits qui y sont inhérents. Cette réforme de nos lois en la matière rétablira la confiance envers la démocratie et l'économie canadiennes.

Éléments supplémentaires pour la réforme des lois sur la protection des renseignements personnels au Canada

Le Commissariat évalue, à l'heure actuelle, des éléments qui seraient essentiels pour moderniser les lois canadiennes sur la protection des renseignements personnels, s'ajoutant à l'intégration d'un cadre fondé sur les droits. Pour ces travaux, nous nous appuyons notamment sur nos dossiers concernant la conformité, la politique et les services-conseils, la modernisation de la législation observée dans la sphère internationale, et des propositions particulières présentées par Innovation, Sciences et Développement économique Canada (ISDE) et par le ministère de la Justice du Canada.

Les paragraphes qui suivent donnent un aperçu de certains enjeux clés que nous explorons actuellement sous l'angle des politiques se rapportant à la modernisation législative.

Plus précisément, nous estimons qu'il faut moderniser les lois canadiennes sur la protection des renseignements personnels pour ce qui suit :

1) Continuer d'accorder une place importante au consentement valable, mais prévoir des solutions de rechange pour protéger la vie privée lorsque l'obtention du consentement n'est pas réaliste.

Sous le régime de la LPRPDE, le principe du consentement est lié à l'autonomie des individus; il leur permet d'exercer un certain contrôle sur le traitement de leurs données. Ainsi, le consentement peut jouer un rôle important dans la protection de la vie privée. Pourtant, nous observons de plus en plus de limites au modèle de consentement dans un environnement où l'on cherche, afin d'innover ou de générer des profits, à utiliser les données à des fins autres que celles pour lesquelles elles ont été recueillies. Cette situation fait en sorte que les individus subissent un fardeau excessif, et un transfert déraisonnable de responsabilité, en raison des demandes de consentement souvent formulées en des termes vagues et incompréhensibles.

Pour ce qui est de la collecte de renseignements personnels par le gouvernement fédéral sous le régime de la LPRP, l'obligation d'obtenir le consentement de l'individu concerné est beaucoup plus limitée que dans la LPRPDE. En vertu de la LPRP, une institution fédérale a le droit de recueillir et d'utiliser les renseignements personnels sans le consentement des intéressés pour autant que ces renseignements aient un lien direct avec ses programmes ou ses activités. L'institution fédérale est tenue d'obtenir le consentement des intéressés pour utiliser ou communiquer leurs renseignements personnels uniquement si elle compte s'en servir à des fins autres que celles auxquelles ces renseignements ont été recueillis ou dans les cas d'exception autorisés en vertu de la Loi.

Nous estimons qu'il devrait toujours y avoir une place dans la loi pour le consentement lorsqu'il s'agit d'un moyen efficace permettant aux individus d'exercer un contrôle sur leurs renseignements. En outre, quand

on demande leur consentement aux individus, celui-ci doit être valable. Nous avons publié en 2018 les Lignes directrices pour l'obtention d'un consentement valable, qui mettent l'accent sur la LPRPDE. Nous y avons souligné plusieurs mesures à prendre afin de s'assurer d'obtenir un consentement valable des intéressés pour recueillir, utiliser ou communiquer leurs renseignements personnels. Pour ne donner que quelques exemples, nous estimons nécessaire que les organisations du secteur privé respectent les principes suivants :

- Fournir aux individus une description des renseignements recueillis plus accessible et en des termes plus faciles à comprendre. Préciser notamment les tiers auxquels les renseignements seront communiqués, les fins auxquelles ceux-ci seront recueillis, utilisés et communiqués, ainsi que les utilisations non essentielles à la prestation des services. Finalement, indiquer aux individus tout risque significatif d'atteinte à leur vie privée découlant du recours aux services fournis.
- Permettre aux individus de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée.
- Concevoir ou adopter des processus de consentement novateurs qui peuvent être mis en œuvre juste à temps, sont adaptés au contexte et conviennent au type d'interface.

Bien que le consentement des individus ait sa place, la loi devrait peut-être autoriser des exceptions à cet égard dans des circonstances limitées définies dans la législation, lorsque les avantages pour la société l'emportent manifestement sur les atteintes à la vie privée et où plusieurs conditions préalables sont respectées avant de pouvoir utiliser les renseignements à ces fins. Certains parlent de « fins socialement bénéfiques » ou de « bien public » afin de désigner les avantages pour la société. Nous estimons qu'il faut un examen plus critique de ce que les entreprises (et les gouvernements) considèrent comme des avantages sociétaux. Notre travail d'enquête et de consultation nous a appris que les utilisations dites socialement bénéfiques par une entreprise, une industrie ou un gouvernement ne correspondent pas toujours à l'idée que le public se fait d'un bien pour la société ou des intérêts individuels – certains avantages sont plus grands que d'autres et

le bon vouloir des individus à mettre leurs droits en péril au nom du bien public a ses limites.

Dans le Rapport sur le consentement paru dans notre Rapport annuel de 2016-2017, nous avons proposé que le Parlement envisage de modifier la LPRPDE afin d'y insérer de nouvelles exceptions au consentement pour permettre des activités d'utilité sociale que les rédacteurs originaux de la LPRPDE n'avaient pas prévues. Nous avons suggéré que toute organisation du secteur privé désirant se prévaloir d'une telle exception devrait respecter plusieurs conditions préalables, dont les suivantes :

- l'utilisation des renseignements personnels est nécessaire;
- l'obtention du consentement est irréalisable en pratique;
- des données pseudonymisées seront utilisées dans la mesure du possible;
- les avantages sociétaux l'emportent manifestement sur les ingérences dans la vie privée;
- une EFVP a été réalisée au préalable;
- l'organisation a avisé le Commissariat au préalable;
- l'organisation a diffusé un avis public décrivant ses pratiques;
- les individus conservent le droit de s'opposer.

Le RGPD prévoit plusieurs fondements juridiques pour le traitement des renseignements personnels, notamment l'« intérêt légitime ». Pour pouvoir invoquer cet intérêt, une organisation doit d'abord expliquer la fin visée et démontrer la nécessité du traitement. Elle doit en outre prouver que ses propres intérêts ne portent pas atteinte aux intérêts, droits ou libertés d'individus. De plus, l'organisation invoquant des intérêts légitimes doit prendre en compte les objections personnelles. Dans certaines circonstances limitées, les autorités publiques peuvent envisager d'invoquer leurs intérêts légitimes comme fondement juridique pour le traitement, mais d'autres fondements juridiques seraient probablement plus appropriés (c.-à-d. le mandat que leur confère la loi).

Dans son document intitulé Renforcer la protection de la vie privée dans l'ère numérique, ISDE souligne

qu'il explore la façon dont les exceptions en matière de consentement pourraient se présenter dans une loi modernisée selon le concept de « pratiques commerciales normalisées » qu'il propose. Le Ministère précise que ce concept pourrait s'appliquer à des fins telles que la prestation d'un service, l'utilisation des renseignements à des fins d'authentification, leur communication à des tierces parties qui les traitent, la gestion du risque, ou le respect d'exigences réglementaires. Selon la description actuelle des « pratiques commerciales normalisées » proposée par ISDE, il s'agit d'un concept ayant une trop grande portée qui pourrait bien devenir une exception fourre-tout, voire une faille énorme. En termes simples, les entreprises ne devraient pas être autorisées à se soustraire à l'obligation d'obtenir le consentement simplement parce qu'elles considèrent qu'une pratique est « normalisée ».

Pour sa part, le ministère de la Justice du Canada se penche sur le rôle du consentement sous le régime de la LPRP, notamment à savoir s'il existe des cas où les individus pourraient vraiment prendre des décisions éclairées et de donner un consentement valide dans le contexte du secteur public. Il examine aussi la meilleure façon d'aider les individus à exercer un contrôle sur leurs renseignements personnels dans le modèle de gouvernance reposant sur des pouvoirs conférés par la LPRP et à donner leur consentement dans ce cadre. Il s'agit de questions fondamentales compte tenu de l'objectif déclaré publiquement par le gouvernement fédéral consistant à passer à un modèle de prestation des services basé sur l'approche « une fois suffit », selon lequel les données entrées dans un système du gouvernement peuvent être réutilisées dans de nombreux autres systèmes du gouvernement.

2) Imposer la norme de nécessité et de proportionnalité pour la collecte de renseignements personnels.

Comme nous l'avons déjà signalé, la LPRP dans sa forme actuelle n'exige pas le consentement pour recueillir des renseignements personnels. En effet, une institution fédérale peut recueillir des renseignements tant et aussi longtemps qu'ils ont un lien direct avec ses programmes ou ses activités. D'après notre expérience, ce pouvoir est parfois exercé de façon trop large. Nous avons signalé au Parlement que le passage à la numérisation a rendu

la collecte, l'utilisation, la communication et la conservation de l'information beaucoup plus faciles pour le gouvernement. L'imposition d'un seuil plus strict pour la collecte de renseignements personnels par le gouvernement en vertu de la LPRP limiterait la collecte excessive de renseignements personnels auprès de citoyens.

Cette tendance au chapitre de la collecte excessive a également été mise en évidence dans notre enquête mettant en cause Statistique Canada, en réponse à des plaintes qui portaient sur la collecte de renseignements personnels de nombreux Canadiens auprès d'une agence d'évaluation du crédit et sur la collecte prévue de renseignements personnels auprès d'institutions financières. Pour régler le problème, le Commissariat a recommandé d'appliquer un critère de nécessité et de proportionnalité à la collecte de renseignements personnels par les institutions fédérales.

L'introduction d'un critère de nécessité et de proportionnalité dans la loi limiterait efficacement le risque de collecte excessive de renseignements personnels au palier fédéral, puisque les initiatives gouvernementales seraient soumises dès le début à une évaluation approfondie visant à détecter les risques d'atteinte à la vie privée. Le principe de nécessité figure déjà dans des lois provinciales et territoriales protégeant les renseignements personnels dans le secteur public. Il s'agit d'une norme généralement acceptée pour éviter la collecte excessive de renseignements personnels par les institutions publiques. Les institutions fédérales seraient tenues de faire état d'un but public pressant et substantiel afin de démontrer la nécessité de la collecte.

La proportionnalité découle non pas du droit administratif, mais du droit en matière de droits de la personne, où il s'agit d'un concept bien connu pour trouver un juste équilibre entre les atteintes aux droits et la protection d'autres droits ou intérêts importants. Ce concept figure aussi dans le RGPD, sous le point 4. En outre, selon une interprétation de la Cour d'appel fédérale, certains aspects de la proportionnalité font partie de la LPRPDE, notamment son paragraphe 5(3). Une obligation de proportionnalité imposée explicitement dans la LPRP limiterait encore davantage la collecte de renseignements personnels par le gouvernement et renforcerait ainsi la protection de la vie privée.

3) Obliger les organisations et les institutions fédérales à faire la preuve de leur responsabilité.

La responsabilité, principe clé en vertu de la LPRPDE, se rapporte au devoir d'une organisation de protéger les renseignements personnels comme l'exige la loi. Tout en considérant la responsabilité comme un principe important de la loi, nous constatons de plus en plus les lacunes à cet égard dans le monde actuel où la circulation des données est complexe et où les modèles d'affaires sont très peu transparents. Par exemple, nos récentes enquêtes sur Facebook et Equifax ont révélé que la responsabilité telle qu'elle est prévue dans la loi ne constitue pas un outil assez puissant pour protéger les Canadiens contre les pratiques envahissantes d'entreprises qui affirment faussement en faire preuve.

Les lacunes de la LPRP sont manifestes comparativement à la série de principes relatifs à l'équité dans le traitement de l'information énoncés dans la LPRPDE. Le ministère de la Justice du Canada examine actuellement à quoi ressemblerait une plus grande responsabilisation dans une loi renouvelée portant sur la protection des renseignements personnels. Dans sa déclaration publique sur la modernisation de la loi sur la protection des renseignements personnels dans le secteur public fédéral du Canada, le ministère de la Justice a fait remarquer, par exemple, qu'une LPRP modernisée devrait « démontrer une responsabilisation significative et transparente, y compris une surveillance efficace ».

En somme, il faut renforcer le cadre de responsabilité actuel.

En nous appuyant sur les leçons tirées d'enquêtes récentes, nous préconisons une loi améliorée et renforcée exigeant une responsabilité démontrable. La loi ne doit pas simplement imposer des obligations en matière de responsabilité, comme c'est le cas en vertu de la LPRPDE, puis laisser les organisations décider elles-mêmes comment elles s'y conformeront. Il s'agirait là d'une autre forme d'autoréglementation, qui s'est avérée inacceptable. Plus précisément, nous proposons d'apporter les améliorations suivantes pour appuyer la responsabilité démontrable :

- **Pouvoir d'inspection proactive sans motifs :** Dans le monde actuel, où les modèles de prestation de services des entreprises et du gouvernement sont opaques et où la circulation de l'information est de plus en plus complexe, il est peu probable que

les gens déposent une plainte s'ils ne sont pas au courant d'une pratique susceptible de leur porter préjudice. C'est pourquoi il est si important que la loi confère à l'organisme de réglementation de la protection de la vie privée le pouvoir d'inspecter de façon proactive les pratiques des organisations. En vertu de l'article 37 de la LPRP, le commissaire peut, à sa discrétion, faire enquête pour s'assurer qu'une institution fédérale se conforme à des articles particuliers de cette loi. L'ajout d'une disposition similaire dans la LPRPDE nous rapprocherait d'un modèle de responsabilité assurée et nous éloignerait du modèle actuel défaillant reposant sur l'autoréglementation dans le secteur privé. Au Royaume-Uni et dans plusieurs autres pays, ces pouvoirs constituent actuellement un mécanisme essentiel à une application efficace de la loi.

- **Obligation de faire sur demande la preuve de la responsabilité :** La loi devrait obliger les organisations et les institutions fédérales à tenir des registres pour prouver qu'elles respectent les exigences de responsabilité. Leur capacité à démontrer une responsabilité véritable devient encore plus importante dans les cas où l'obtention du consentement est irréalisable en pratique ou qu'elle n'est pas exigée; on s'attend dans ces cas à ce que les organisations et les institutions fédérales combleront, grâce à la responsabilité, les lacunes en matière de protection. L'obligation de tenir des registres serait nécessaire afin que le Commissariat ait la capacité d'effectuer des inspections proactives sous le régime de la LPRPDE, comme nous l'avons expliqué. Nous avons observé ce manque dans nos travaux portant sur la conformité sous le régime de la LPRP.

Une responsabilité démontrable fait également partie de la solution pour protéger les Canadiens dans le contexte de la circulation transfrontalière des données. Notre enquête sur Equifax a démontré que le principe de responsabilité tel qu'il est formulé actuellement dans la LPRPDE n'est pas toujours efficace pour protéger les Canadiens dans un contexte transfrontalier. Afin d'y remédier, la loi doit prévoir à tout le moins un régime de responsabilité plus solide, par l'adoption d'une responsabilité démontrable, et possiblement d'autres mesures supplémentaires,

telles que les clauses contractuelles types du régime européen. Nous constatons qu'ailleurs, des propositions créatives sont présentées pour améliorer la protection de la vie privée des consommateurs en renforçant les obligations d'une entreprise à l'égard de ses clients. Par exemple, le projet de loi de l'État de New York sur la protection de la vie privée a introduit le concept de fiduciaire des données, ce qui signifie que les entreprises auraient la responsabilité de protéger les renseignements personnels de leurs clients et seraient sanctionnées si elles agissaient d'une manière qui ne protège pas les intérêts des personnes.

- **Obligation de tenir compte du droit à la vie privée dès la conception et d'évaluer les risques d'atteinte à la vie privée au début de la planification :**

La responsabilité exige l'assurance que le droit à la vie privée est pris en compte tout au long du cycle de vie d'un produit, d'un service ou d'une initiative – depuis la conception initiale jusqu'au déploiement et à la mise en œuvre à long terme. Le concept de « vie privée dès la conception », élaboré par Ann Cavoukian alors qu'elle était commissaire à l'information et à la protection de la vie privée de l'Ontario, s'avère utile à cet égard. Nous considérons que les EFVP constituent un outil efficace pour appuyer cette exigence de protection de la vie privée dès la conception. D'ailleurs, le Commissariat a réclamé à plusieurs occasions que les EFVP fassent l'objet d'une exigence imposée dans la loi. Nous constatons que plusieurs instances européennes exigent la protection des données dès la conception et au moyen de mesures par défaut. Une surveillance exercée par une autorité de protection des données ou une exigence de mener une évaluation des facteurs relatifs à la protection des données (similaire à l'EFVP en place au Canada) permettent d'en assurer la mise en œuvre. Nombre de lois en vigueur en dehors de l'Union européenne comprennent, elles aussi, l'obligation de protéger les données dès la conception, ainsi que des mesures par défaut.

Il faut imposer aux organisations et aux institutions fédérales des exigences plus strictes en matière de responsabilité pour contribuer à une protection de la vie privée véritable à l'ère du numérique. Ces exigences

doivent suivre le même rythme de croissance que la communication des renseignements personnels, notamment au-delà des frontières nationales, dans le cadre de la fourniture de produits et de services. Dans cet exercice de renforcement de la responsabilité, il faut tenir compte, selon nous, des intérêts des petites et moyennes entreprises (PME). Certes, les principes d'une nouvelle loi sur la protection de la vie privée devraient s'appliquer à toutes les organisations, quelle que soit leur taille, mais la façon dont ces principes sont appliqués peut varier pour les PME. Par exemple, les obligations en matière de tenue de registres, en vertu du principe de responsabilité, pourraient être allégées pour les PME, à moins que ces dernières mènent des activités qui comportent des risques substantiels pour la vie privée.

- 4) **Conférer à une autorité publique le pouvoir de publier des lignes directrices contraignantes pour assurer une bonne compréhension pratique des exigences imposées par la loi et pour apporter une certitude aux individus, aux organisations et aux institutions fédérales.**

La LPRPDE est une loi fondée sur des principes et formulée de façon très générale, ce qui présente des avantages dans un secteur qui évolue rapidement, comme celui de la technologie, puisqu'elle peut s'appliquer dans des circonstances que l'on n'avait peut-être pas prévues au moment de sa rédaction. En revanche, il est parfois difficile dans la pratique d'appliquer avec une grande certitude de telles lois formulées de façon à présenter un certain niveau d'abstraction. D'autres mécanismes devraient être en place pour donner une dimension plus concrète aux principes généraux. Des instruments efficaces pour aider à interpréter la loi peuvent notamment prendre la forme de lignes directrices obligatoires, de règlements et d'ordonnances exécutoires.

Un modèle possible serait qu'une autorité publique ait le pouvoir de publier des lignes directrices contraignantes en vertu de la LPRPDE, ce qui aiderait à préciser la façon d'appliquer dans la pratique les principes généraux de cette loi. L'autorité publique en question pourrait être le Commissariat, un ministère fédéral, ou une autre entité de l'État. Des lignes directrices contraignantes assureraient une compréhension plus pratique des exigences de la loi. En outre, on pourrait les modifier

plus facilement que la loi elle-même en fonction de l'évolution de la technologie et des pratiques. Une autre option serait de s'en remettre au pouvoir de rendre des ordonnances du Commissariat pour élaborer des lignes directrices contraignantes par l'entremise des ordonnances prises dans des cas particuliers.

ISDE a proposé de favoriser, dans une réforme de la loi sur la protection des renseignements personnels dans le secteur privé, l'élaboration de codes de pratique, de régimes d'accréditation et de certification, et de normes comme moyen de faire preuve de diligence raisonnable en ce qui concerne la conformité à certaines dispositions de cette loi. Le Ministère précise qu'il faut reconnaître l'importance et l'utilité des normes, des codes et de la certification en tant qu'outils à l'appui des « règles » de protection de la vie privée, et comme moyen d'encourager la conformité et de contribuer potentiellement à l'adoption d'un modèle d'application plus proactif. Tout en étant ouverts à ce type de régime en principe, nous croyons fermement que si ces instruments se veulent exécutoires, l'autorité chargée de leur élaboration et de leur approbation doit être une entité de l'État indépendante de l'industrie. On ne peut laisser les entreprises définir elles-mêmes les règles, ce qui perpétuerait forcément le modèle d'autoréglementation actuel. Tout système non contraignant d'incitation au respect de la loi serait le bienvenu, mais il ne devrait pas être confondu avec la loi.

5) Autoriser le Commissariat à choisir les plaintes sur lesquelles faire enquête, tout en s'assurant que les individus bénéficient d'un droit privé d'action.

À l'heure actuelle, la LPRP ne confère pas au commissaire le pouvoir de refuser d'examiner une plainte ou de mettre fin à son examen. Or, la LPRPDE lui accorde ce pouvoir dans certaines circonstances particulières. Nous avons recommandé au Parlement de conférer au Commissariat le pouvoir de choisir les plaintes sur lesquelles faire enquête de manière à concentrer ses ressources limitées sur les questions présentant le risque le plus élevé ou pouvant avoir le plus de répercussions pour les Canadiens. Afin que personne ne soit sans recours en cas d'infraction à la loi, nous avons aussi recommandé d'accorder aux individus un droit privé d'action.

À l'instar de nombreuses autres autorités de protection de la vie privée et des données, le Commissariat doit s'acquitter de plusieurs mandats en disposant de ressources limitées. Lorsque nous ne faisons pas enquête sur une plainte déposée par un individu, le plaignant devrait avoir le droit d'intenter des poursuites de son propre chef. Ainsi, les individus ne seraient pas laissés sans recours et ils pourraient plus facilement faire respecter leurs droits. Ce droit est établi dans le RGPD et envisagé par d'autres instances. Par exemple, la *New York privacy act*, qui était à l'étude au comité sénatorial de l'État sur la protection des consommateurs au moment de la rédaction du présent rapport, vise à conférer aux individus le droit, entre autres, de poursuivre eux-mêmes en justice les entreprises qui portent atteinte à leur vie privée.

6) Autoriser le partage d'information entre des organismes de réglementation ayant des mandats différents.

De toute évidence, une protection efficace des consommateurs et des citoyens à l'ère du monde numérique et de l'économie axée sur les données, où tout va vite, doit faire intervenir plusieurs organismes de réglementation qui peuvent coordonner et partager leurs travaux. Une loi modernisée doit permettre, dans certaines circonstances, l'échange d'information entre différents organismes de réglementation afin d'assurer une meilleure coordination de leurs travaux. Ce changement s'impose : le mandat des organismes de réglementation se chevauche parfois au cours d'une enquête, mais ces derniers n'ont pas l'autorisation d'échanger l'information pertinente. Cette interdiction porte préjudice aux Canadiens et entraîne un manque d'efficacité qui pourrait potentiellement retarder les recours des individus. Un tel changement pourrait contribuer à faire en sorte que les Canadiens disposent du recours le plus efficace possible, en s'appuyant sur l'expertise différente des divers organismes de réglementation. Il pourrait aussi permettre au Commissariat de venir en aide à divers autres organismes de réglementation ne possédant aucune expertise dans le domaine en leur donnant de l'information concernant les répercussions de leurs décisions sur la vie privée. Compte tenu de l'utilisation généralisée des renseignements personnels dans tous les secteurs, la protection de la vie privée constitue de plus en plus une question transversale.

7) Veiller à ce que la loi s'applique à l'ensemble du gouvernement fédéral et aux partis politiques fédéraux.

À l'heure actuelle, la LPRP ne s'applique qu'aux institutions mentionnées à l'annexe 1 de la Loi et à celles répondant à la définition d'« institution fédérale » énoncée dans la section « Définitions » (par exemple les sociétés d'État). Nous recommandons de modifier cette loi de sorte qu'elle s'applique à toutes les institutions fédérales ainsi qu'aux cabinets des ministres et à celui du premier ministre. Comme la loi actuelle ne s'applique pas à l'ensemble du gouvernement, nous nous sommes heurtés à des obstacles dans le cadre d'enquêtes sur une plainte dont la portée englobait des institutions non visées. Un élargissement du champ d'application de la loi permettrait au Commissariat d'exercer une surveillance plus efficace. En outre, le gouvernement dans son ensemble serait assujéti à la même série de règles.

De plus, les partis politiques fédéraux doivent être explicitement assujettis aux lois sur la protection des renseignements personnels. Le scandale Facebook / Cambridge Analytica nous a récemment montré que les partis politiques recueillent de grandes quantités de renseignements personnels sur les électeurs alors qu'ils adoptent des techniques de microciblage. Ces pratiques font la preuve du lien inextricable entre le droit à la vie privée et la démocratie. En particulier, il révèle comment on peut utiliser des renseignements personnels à notre sujet pour influencer sur notre réflexion et nos actions et ainsi entraver nos processus démocratiques. Nous avons récemment publié des *Conseils sur la protection des renseignements personnels pour les partis politiques fédéraux*, mais il s'agit d'un document d'orientation non contraignant. Il faut absolument renforcer les mesures de protection de la vie privée et assujettir les partis politiques à la règle de droit.

8) Prévoir des mesures de protection supplémentaires contre les préjudices découlant d'atteintes aux droits de la personne à l'ère du numérique.

En raison des mégadonnées, de l'intelligence artificielle, de la prise de décisions automatisée et du profilage des données, il faut absolument améliorer la protection de la vie privée des individus pour assurer le respect de leurs droits fondamentaux à l'ère du numérique. Nous constatons qu'ailleurs dans le monde, des instances ont rapidement pris des mesures afin que la loi prenne en compte les risques propres à notre réalité numérique, notamment le droit à l'oubli, le droit à la portabilité des données, et les droits en matière de transparence et d'explication quant à l'algorithme. Bien entendu, ces droits renforcés protégeant la vie privée doivent être en harmonie avec les autres droits constitutionnels. Par exemple, le droit à l'oubli et la liberté d'expression doivent être pris en compte simultanément.

Le Projet de position du Commissariat sur la réputation en ligne présente notre point de vue préliminaire en ce qui concerne la réputation en ligne, notamment le droit à l'oubli. Cette prise de position initiale, qui prend en compte les mesures de protection existantes et les lacunes des lois fédérales sur la protection des renseignements personnels dans le secteur privé, prévoit ce qui suit : le droit de demander aux moteurs de recherche le déréférencement de pages Web qui renferment des renseignements inexacts, incomplets ou périmés; la suppression ou la modification de renseignements à la source; ainsi que la sensibilisation du public pour aider les Canadiens à devenir des cybercitoyens responsables et bien informés.

Le Commissariat a en outre demandé un renvoi à la Cour fédérale pour déterminer si le moteur de recherche Google est assujéti à la LPRPDE, question qui a été soulevée dans le contexte d'une plainte reçue par le Commissariat contre Google dans laquelle le plaignant demandait que certaines pages Web soient déréférencées des résultats produits par une recherche de son nom. Bien que cette question de compétence soit présentement devant les tribunaux, nous estimons qu'il en revient au Parlement de se pencher sur le droit à l'oubli et sur d'autres mécanismes de protection éventuels de la réputation en ligne, et qu'il serait inapproprié d'attendre avant d'agir devant des questions aussi fondamentales.

Pour en savoir davantage

Lignes directrices pour l'obtention d'un consentement valable

« Rapport sur le consentement », Rapport annuel au Parlement 2016-2017

New York State Senate Bill S5642, *New York privacy act* (en anglais seulement)

« Refus d'enquêter » et « mettre fin à l'examen » en vertu de la LPRPDE

Conseils sur la protection des renseignements personnels pour les partis politiques fédéraux

Projet de position du Commissariat sur la réputation en ligne

En somme, selon nous, une législation modernisée doit établir des droits assurant une protection contre les atteintes propres à l'ère numérique, sans toutefois se limiter à la surveillance généralisée, à la discrimination par suite du profilage, à la prise de décisions automatisée et à l'analyse des données sur le comportement. Nous sommes convaincus que l'industrie et le gouvernement pourront continuer de créer des services utiles à l'intention des Canadiens et d'en tirer parti dans un monde où la loi reconnaît et protège tous les droits des Canadiens.

Conclusion

Nos lois n'ont tout simplement pas évolué au même rythme que l'environnement auquel elles s'appliquent. Dans notre réalité actuelle, de nouveaux modèles d'affaires misant sur les renseignements personnels émergent chaque jour et l'accumulation de renseignements personnels est de plus en plus considérée comme un avantage concurrentiel. Il s'agit d'une réalité où les individus, les entreprises et le gouvernement cherchent tous à exploiter les avantages de la technologie, bien souvent sans pleinement comprendre les risques en découlant. Combiné à la facilité avec laquelle l'information circule en traversant les frontières et change de main, ce recours accru à la technologie fait en sorte que les individus peuvent difficilement savoir s'ils traitent avec un humain ou un robot, une entité au Canada ou à l'étranger, ou encore le secteur public ou privé.

Ce qui est clair dans cet environnement numérique complexe, c'est que nos lois sur la protection des renseignements personnels doivent être adaptées aux réalités d'aujourd'hui et garantir plus vigoureusement les droits des Canadiens. Le moment est venu de passer à l'action.

Supplément à « Réforme des lois sur la protection des renseignements personnels »

On trouvera ci-après des préambules et énoncés d'objet modèles qui serviraient à asseoir le droit à la vie privée dans le cadre qui lui est propre, soit celui des droits de la personne.

Ces libellés serviraient à définir les valeurs, principes et objectifs qui devraient guider l'interprétation et l'application de la LPRPDE et de la LPRP.

Nous recommandons qu'à la fois un préambule et un énoncé d'objet apparaissent au début de chacune des deux lois.

Libellé proposé pour la LPRPDE

Préambule

ATTENDU QUE la protection de la vie privée est un droit fondamental de chaque personne et une valeur fondamentale protégée dans les instruments internationaux portant sur les droits de la personne dont le Canada est signataire;

ATTENDU QUE le droit à la vie privée protège l'autonomie et la dignité individuelles et est lié à la protection de la réputation et à la liberté de pensée et d'expression;

ATTENDU QUE la protection de la vie privée est nécessaire au maintien de relations de confiance mutuelle qui sont essentielles au tissu social canadien;

ATTENDU QUE la protection de la vie privée est essentielle à la préservation de la démocratie ainsi qu'à la pleine jouissance et à l'exercice de bon nombre des droits et libertés garantis par la *Charte canadienne des droits et libertés*;

ATTENDU QUE le contexte technologique actuel et en constante évolution facilite la collecte de quantités massives de données personnelles ainsi

que l'utilisation de ces données, qu'elles soient identifiables, agrégées ou rendues anonymes, d'une manière qui peut avoir des répercussions négatives sur les personnes, les groupes et les communautés;

ATTENDU QUE le traitement des données personnelles doit être conçu pour servir l'humanité;

ATTENDU QUE le traitement responsable des données personnelles peut servir des intérêts publics tels que la croissance économique, l'amélioration des soins de santé et la protection de l'environnement;

ATTENDU QUE cette loi protège le droit à la vie privée des personnes tout en reconnaissant l'intérêt légitime des organisations à recueillir, à utiliser et à communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances et d'une manière qui ne constitue pas de la surveillance;

ATTENDU QUE le droit à la vie privée doit être mis en équilibre avec d'autres droits fondamentaux comme le droit à la liberté d'expression dans des circonstances où la collecte, l'utilisation ou la communication de renseignements personnels sert un intérêt public légitime;

ET ATTENDU QUE cette loi a été reconnue par les tribunaux comme étant de nature quasi constitutionnelle;

Objet

La présente loi a pour objet :

- (a) de mettre en œuvre le droit fondamental à la vie privée des individus dans le contexte commercial au moyen d'une solide protection des données qui garantit que le traitement des données est licite, équitable, proportionnel, transparent et responsable, et respecte les droits et libertés fondamentaux de la personne;
- (b) d'établir un équilibre entre le droit à la vie privée et le droit à la liberté d'expression dans des circonstances où la collecte, l'utilisation ou la communication de renseignements personnels sert un intérêt public légitime;

- (c) d'établir un équilibre, le cas échéant, entre le droit à la vie privée et ce qu'exige l'intérêt public;
- (d) de protéger le droit à la vie privée des personnes tout en reconnaissant l'intérêt légitime des organisations à recueillir, à utiliser et à communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances et d'une manière qui ne constitue pas de la surveillance;
- (e) d'offrir aux personnes des recours rapides et efficaces lorsque leur droit à la vie privée n'est pas respecté et de veiller à ce que les organisations s'acquittent en permanence de leurs obligations prévues dans la présente Loi.

Libellé proposé pour la LPRP

Préambule

ATTENDU QUE la protection de la vie privée est un droit fondamental de chaque personne et une valeur fondamentale protégée dans les instruments internationaux portant sur les droits de la personne dont le Canada est signataire;

ATTENDU QUE le droit à la vie privée protège l'autonomie et la dignité individuelles et est lié à la protection de la réputation et à la liberté de pensée et d'expression;

ATTENDU QUE la protection de la vie privée est nécessaire au maintien de relations de confiance mutuelle qui sont essentielles au tissu social canadien;

ATTENDU QUE la protection de la vie privée est essentielle à la préservation de la démocratie ainsi qu'à la pleine jouissance et à l'exercice de bon nombre des droits et libertés garantis par la *Charte canadienne des droits et libertés*;

ATTENDU QUE le contexte technologique actuel et en constante évolution facilite la collecte de quantités massives de données personnelles ainsi que l'utilisation de ces données, qu'elles soient

identifiables, agrégées ou rendues anonymes, d'une manière qui peut avoir des répercussions négatives sur les personnes, les groupes et les communautés;

ATTENDU QUE toutes les personnes ont le droit constitutionnel à la protection contre les fouilles, perquisitions ou saisies abusives, y compris le droit à la protection contre une surveillance injustifiée par l'État;

ATTENDU QUE le gouvernement fédéral doit uniquement recueillir, utiliser ou communiquer des renseignements personnels de façon licite, équitable, proportionnelle, transparente et responsable, et seulement pour servir les intérêts des Canadiens ou l'intérêt public légitime;

ATTENDU QUE cette loi a été reconnue par les tribunaux comme étant de nature quasi constitutionnelle;

Objet

La présente loi a pour objet :

- (a) de mettre en œuvre le droit fondamental à la vie privée des individus à l'égard de leurs renseignements personnels dans le secteur public fédéral au moyen d'une solide protection des données qui garantit que le traitement des renseignements personnels est licite, équitable, proportionnel, transparent et responsable, et respecte les droits et libertés fondamentaux de la personne;
- (b) d'établir un équilibre entre le droit à la vie privée des personnes et l'obligation du gouvernement de recueillir, d'utiliser et de communiquer des renseignements personnels à des fins qui servent manifestement l'intérêt public;
- (c) d'offrir aux personnes des recours rapides et efficaces lorsque leur droit à la vie privée n'est pas respecté et de veiller à ce que les institutions s'acquittent en permanence de leurs obligations légales prévues dans la présente Loi.

Activités parlementaires

Le droit à la vie privée est une valeur intemporelle. Cela dit, la protection de la vie privée suscite aujourd'hui beaucoup plus de préoccupations auprès des Canadiens qu'en 1983, année où le Commissariat a été établi. Moins d'une génération plus tard, des percées technologiques spectaculaires ont métamorphosé les interactions entre les entreprises et les consommateurs, et entre l'État et les citoyens. L'économie et le gouvernement numériques ont ouvert la voie à de grandes améliorations, mais ont entraîné dans leur sillage des risques importants, qui se réalisent sous forme d'atteintes massives à la sécurité des données et de surveillance omniprésente.

À la lumière de ce changement sociétal, les parlementaires s'appuient de plus en plus souvent sur nos conseils d'experts pour l'examen de projets de loi qui auront des répercussions importantes sur les droits des Canadiens. En effet, des membres du Commissariat ont comparu devant le Parlement plus souvent au cours de l'année civile 2018 qu'au cours de toute autre parmi nos 35 années d'existence.

La section qui suit présente un résumé des conseils que nous avons formulés au Parlement en 2018-2019 à l'occasion de diverses études en comité.

Législation

Projet de loi C-76, Loi sur la modernisation des élections

Avec en toile de fond la controverse que suscite partout dans le monde l'ingérence étrangère dans le processus démocratique, le projet de loi C-76, *Loi sur la modernisation des élections*, est venu proposer des modifications aux procédures et processus électoraux fédéraux.

Malheureusement, la Loi n'assujettit toujours pas les partis politiques fédéraux aux lois sur la protection des renseignements personnels. La Loi a imposé une nouvelle exigence les obligeant à élaborer une politique de confidentialité par écrit, ce que la plupart des partis nationaux avaient déjà fait. Certes, le contenu en est prescrit, mais rien n'exige qu'en substance cette politique soit conforme aux normes internationales en la matière.

Nous avons recommandé que les partis politiques fédéraux soient tenus de respecter les principes de protection de la vie privée reconnus à l'échelle internationale et qu'un tiers indépendant soit habilité à vérifier la conformité à ces principes. Nos recommandations n'ont pas été retenues.

Les partis politiques ont le loisir d'établir la norme à laquelle ils veulent se conformer. Au final, la *Loi sur la modernisation des élections* n'améliore pas la protection de la vie privée.

Il convient de noter que les partis politiques sont assujettis à des lois sur la protection de la vie privée dans de nombreux territoires de compétence partout dans le monde, notamment l'Union européenne, le Royaume-Uni, la Nouvelle-Zélande, l'Argentine et Hong Kong. Fait à signaler également, 92 % des répondants à un sondage que nous avons mené il y a 10 ans étaient d'avis que les partis politiques devraient être assujettis à une forme quelconque de loi sur la protection de la vie privée.

En avril 2019, de concert avec le directeur général des élections, le Commissariat a fourni des conseils sur la protection des renseignements personnels à l'intention des partis politiques fédéraux. Ce document d'orientation a été rédigé pour aider les partis à se conformer aux nouvelles exigences juridiques visant

les politiques de confidentialité. On y propose également des pratiques exemplaires que les partis peuvent adopter pour mieux protéger les renseignements personnels et favoriser la confiance des Canadiens.

Pour en savoir davantage

[Projet de loi C-76, Loi sur la modernisation des élections](#)

[Déclaration de Daniel Therrien, Comparution devant le Comité permanent de la procédure et des affaires de la Chambre pour discuter de l'étude du projet de loi C-76, Loi sur la modernisation des élections](#)

[Sondage auprès des Canadiens de 2009, figure 5.10 : Accord que les partis politiques soient assujettis à une loi sur la vie privée](#)

[Conseils sur la protection des renseignements personnels pour les partis politiques fédéraux](#)

Dans son rapport sur le projet de loi C-74, le Comité a porté la question de la réforme législative à l'attention du gouvernement fédéral pour une étude ultérieure. Tout en reconnaissant que la LPRPDE dépassait la portée de leur étude, les membres du Comité ont fait valoir qu'il fallait mettre à jour les lois canadiennes sur la protection de la vie privée et « les harmoniser avec les normes internationales en la matière ».

Depuis cette comparution, le Commissariat a discuté avec Finances Canada des mesures envisagées par ce ministère. Nous attendons avec intérêt la poursuite de ces discussions.

Pour en savoir davantage

[Projet de loi C-74, Loi n° 1 d'exécution du budget de 2018](#)

[Déclaration de Daniel Therrien, Comparution devant le Comité sénatorial permanent des banques et du commerce concernant la section 16 de la partie 6 du projet de loi C-74](#)

[Lignes directrices pour l'obtention d'un consentement valable](#)

[Lettre de suivi au Comité sénatorial permanent des banques et du commerce concernant le projet de loi C-74, Loi n° 1 d'exécution du budget de 2018](#)

[Rapport du Comité sénatorial permanent des banques et du commerce sur la teneur du Projet de loi C-74](#)

Projet de loi C-74, Loi n° 1 d'exécution du budget de 2018

Le commissaire a comparu devant le Comité sénatorial permanent des banques et du commerce pour l'étude du projet de loi C-74, *Loi n° 1 d'exécution du budget de 2018*. Ce projet de loi prévoyait des modifications visant à éliminer des obstacles à la collaboration entre les institutions financières sous réglementation fédérale et les organisations du secteur des technologies financières.

Le commissaire a indiqué que le gouvernement semblait concentrer ses efforts sur la recherche de l'innovation sans se soucier de la protection de la vie privée. Par exemple, il était difficile de savoir si un consentement serait exigé conformément à nos Lignes directrices pour l'obtention d'un consentement valable. Le commissaire a également souligné qu'il n'avait pas le pouvoir d'obliger les organisations à appliquer des mesures raisonnables en ce qui a trait au consentement.

Dans une lettre de suivi adressée au Comité, le commissaire a proposé une amélioration des dispositions de la LPRPDE qui traitent de l'obligation d'obtenir un consentement valable. Il a aussi proposé l'adoption de nouvelles dispositions permettant au Commissariat de rendre des ordonnances exécutoires à l'encontre des organisations qui ne respectent pas les exigences de cette loi.

Projet de loi C-59, Loi concernant des questions de sécurité nationale

Dans le rapport annuel 2017-2018, on pouvait lire que le Commissariat avait comparu devant le Comité permanent de la sécurité publique et nationale de la Chambre des communes lors de l'étude du projet de loi C-59, puis envoyé des lettres de suivi au Comité à ce sujet. En avril 2019, le commissaire a comparu devant le Comité sénatorial permanent de la sécurité nationale et de la défense dans le contexte de son étude du projet de loi modifié.

Les modifications adoptées par la Chambre des communes introduisent un critère de nécessité raisonnable pour la transmission de renseignements entre institutions chargées de la sécurité nationale.

Le commissaire s'est dit généralement satisfait de ces modifications, qui ont un résultat très similaire à celles qu'il avait recommandées, bien qu'elles y arrivent de manière un peu différente.

Pour ce qui est de la transmission de renseignements confidentiels entre organismes de surveillance, le projet de loi modifié confère au Commissariat l'autorité de partager des renseignements et de coordonner ses activités avec l'Office de surveillance des activités en matière de sécurité, mais non avec le Comité des parlementaires sur la sécurité nationale et le renseignement.

Bien qu'imparfait, le projet de loi finalement adopté par le Parlement demeure raisonnablement équilibré et constitue clairement une amélioration par rapport à la loi précédente.

Pour en savoir davantage

Projet de loi C-59, Loi concernant des questions de sécurité nationale

Déclaration de Daniel Therrien, Comparution devant le Comité permanent de la sécurité publique et nationale au sujet du projet de loi C-59, Loi concernant des questions de sécurité nationale

Déclaration de Daniel Therrien, Comparution devant le Comité sénatorial permanent de la sécurité nationale et de la défense sur le projet de loi C-59, Loi concernant des questions de sécurité nationale

Études parlementaires

En plus d'étudier les projets de loi, les comités parlementaires se sont penchés sur diverses questions ayant une incidence sur la protection de la vie privée, entre autres les dossiers présentés ci-après.

Services gouvernementaux numériques

Le commissaire et d'autres membres de la haute direction du Commissariat ont comparu devant le Comité ETHI dans le cadre de l'étude des répercussions sur la protection de la vie privée et des obstacles juridiques éventuels découlant de la mise en œuvre de services gouvernementaux numériques au palier fédéral. À l'issue de cette étude, le Comité a recommandé au gouvernement des mesures pour améliorer ses services tout en protégeant la vie privée et la sécurité des Canadiens.

Dans notre déclaration, nous avons fait référence à la Feuille de route de la Stratégie de données pour la fonction publique fédérale publiée par le gouvernement en novembre 2018. Ce document propose des modifications à la façon dont la fonction publique fédérale recueille, gère et régit les données. Nous avons fait valoir que ce qui est un obstacle juridique pour certains peut être considéré par d'autres comme une garantie de protection de la vie privée. Nous avons demandé au Comité de se rappeler que, bien que ces rajustements puissent être souhaitables, toute nouvelle législation conçue pour faciliter les services gouvernementaux numériques doit respecter la vie privée en tant que droit de la personne.

Nous avons également formulé des commentaires sur le modèle estonien, dont on parle souvent en raison de son architecture technologique. Nous avons fait remarquer que l'élimination des cloisonnements dans les fonds de renseignements du gouvernement d'Estonie n'a pas abouti à une gestion horizontale tous azimuts des renseignements personnels à l'échelle du gouvernement. Dans ce modèle, la communication des renseignements semble plutôt fondée sur des lois prévoyant des modalités qui cadrent généralement avec les principes relatifs aux pratiques équitables de traitement de l'information reconnus à l'échelle internationale et avec le RGPD de l'Union européenne.

Par ailleurs, dans le modèle estonien, l'autorité chargée de la protection des données joue un rôle important; elle possède le pouvoir de rendre des ordonnances contraignantes, de demander que l'on intente des poursuites criminelles et d'imposer des amendes lorsque le traitement contrevient à la loi ou que les exigences en matière de gestion ou de protection des données ne sont pas respectées. Nous avons recommandé que le Commissariat joue un rôle de surveillance proactif tout aussi important, comme nous l'avons préconisé dans notre déclaration concernant la réforme de la LPRP. Le meilleur moyen à la disposition du Canada pour devenir un chef de file de l'innovation numérique consiste à montrer comment l'on peut établir un cadre pour l'innovation qui protège comme il se doit les valeurs et les droits canadiens ainsi que notre démocratie.

Pour en savoir davantage

[Déclaration de Daniel Therrien, Comparution devant le Comité ETHI concernant la protection des données personnelles dans les services gouvernementaux numériques](#)

[Bureau du Conseil privé, Feuille de route de la Stratégie de données pour la fonction publique fédérale](#)

Grand Comité international sur les mégadonnées, la protection des renseignements personnels et la démocratie

Partout dans le monde, des assemblées législatives sont aux prises avec les répercussions d'un environnement numérique complexe sur les processus et institutions démocratiques. Le Canada a accueilli en mai 2019 un Grand Comité international de parlementaires à la recherche de solutions à ces défis dans la foulée des enquêtes portant sur Facebook et Cambridge Analytica et des révélations troublantes en découlant.

Ce grand comité, composé de représentants de 11 pays, a déclaré que les plateformes de médias sociaux devraient renforcer les droits reliés à la vie privée et les mesures de protection des données, et que la réglementation pourrait être nécessaire à cette fin, notamment pour prévenir les activités numériques qui menacent la paix sociale et interfèrent dans les processus ouverts et démocratiques.

Les témoins qui ont comparu devant ce comité ont abordé des enjeux concernant les mégadonnées, la protection de la vie privée et la démocratie. Au cours des trois jours de témoignage, on a débattu de grandes questions telles le capitalisme de surveillance, le pouvoir de la technologie et des données, la désinformation, la transparence algorithmique, l'économie de l'attention, et le discours haineux en ligne. Les membres du comité ont également entendu des témoignages liés à des sujets pratiques comme le fonctionnement des grandes plateformes, les changements dans l'utilisation d'Internet, et le rôle des tiers et intermédiaires dans la collecte et l'utilisation des données personnelles.

Le commissaire Therrien figurait parmi les spécialistes que le Grand Comité avait invités à comparaître. Il a exhorté les États et les représentants internationaux à ne pas se limiter aux questions de protection des données et de la vie privée malgré leur importance vitale. Il a fait valoir que les institutions démocratiques sont maintenant en butte à la méfiance et à la suspicion, et que la confiance des citoyens envers le processus électoral est ébranlée. Le commissaire a souligné que les outils numériques permettant de faire participer une nouvelle génération de citoyens au processus électoral sont aussi utilisés de plus en plus pour bafouer la démocratie et non pour la renforcer.

À l'instar d'autres témoins, le commissaire a souligné que des approches réglementaires modernisées, des lois plus strictes et une responsabilité démontrable sont d'une importance cruciale pour rétablir la confiance des citoyens.

Pour en savoir davantage

[Déclaration de Daniel Therrien, Comparution devant le Grand Comité international sur les mégadonnées, la protection des renseignements personnels et la démocratie](#)

Système bancaire ouvert

Des représentants du Commissariat ont comparu à deux reprises devant le Comité sénatorial permanent des banques et du commerce à l'occasion de son étude du système bancaire ouvert. Le Commissariat a également présenté un mémoire à Finances Canada dans le cadre de ses consultations sur le système bancaire ouvert.

Dans un système bancaire ouvert, les consommateurs et les entreprises peuvent communiquer des renseignements financiers à un plus grand nombre de fournisseurs de services en contrepartie de services financiers.

Le Commissariat a insisté sur la nécessité de renforcer la confiance envers l'économie numérique et de s'assurer que les personnes ne sont pas considérées comme une marchandise. Le commissaire Therrien a fait remarquer que la protection de la vie privée n'est pas un droit auquel on peut renoncer à la légère au profit de l'innovation, de l'efficacité ou de gains commerciaux.

Plus précisément, nous avons réclamé la mise en place de règles de base uniformes pour le système bancaire ouvert et recommandé l'établissement de normes, y compris de normes techniques et de normes relatives à la protection de la vie privée. Nous avons aussi indiqué que le Commissariat serait heureux de fournir une expertise en matière de protection de la vie privée afin d'appuyer l'élaboration des normes canadiennes. De plus, nous nous sommes dits favorables au modèle selon lequel les nouveaux acteurs doivent obtenir une accréditation et une autorisation avant de participer à une initiative de services bancaires ouverts.

Nous avons aussi recommandé que tout cadre stratégique ou législatif élaboré à l'appui d'un système bancaire ouvert renvoie explicitement au cadre législatif existant en matière de protection de la vie privée au Canada et que le Commissariat exerce une surveillance dans le domaine.

En outre, le Commissariat a souligné qu'il est essentiel que les entreprises exerçant leurs activités dans l'économie numérique respectent ses Lignes directrices pour l'obtention d'un consentement valable.

Nous avons exprimé notre volonté d'appuyer le gouvernement et de collaborer avec lui dans la mise en œuvre de nos recommandations et d'aider aux discussions à venir concernant la planification, la mise en œuvre et la surveillance d'un système bancaire ouvert, y compris l'élaboration des normes nécessaires pour faciliter la communication d'information.

Pour en savoir davantage

Déclaration de Gregory Smolynec, Comparution devant le Comité sénatorial permanent des banques et du commerce au sujet du système bancaire ouvert, février 2019

Déclaration de Gregory Smolynec, Comparution devant le Comité sénatorial permanent des banques et du commerce au sujet du système bancaire ouvert, mai 2019

Examen des mérites d'un système bancaire ouvert : Mémoire à l'intention du Ministère des Finances Canada

Lignes directrices pour l'obtention d'un consentement valable

La Loi sur la protection des renseignements personnels (LPRP)

Rétrospective de l'exercice

La section qui suit présente certaines initiatives clés menées par le Commissariat sous le régime de la LPRP.



La LPRP accuse son âge. Ce fait est ressorti clairement dans certaines de nos enquêtes, où nous avons constaté que la Loi n'est pas toujours à la hauteur des défis de l'ère numérique.

Au moment de l'entrée en vigueur de la Loi il y a plus de 30 ans, nombre des questions qui étaient au cœur des enquêtes menées en 2018-2019 en vertu de la LPRP (par exemple, l'examen des appareils mobiles par des agents frontaliers et l'acquisition de renseignements personnels par des ministères auprès de courtiers en données) relevaient encore de la science-fiction.

En particulier, notre enquête sur les initiatives de collecte massive de données à Statistique Canada a fait ressortir l'urgence de moderniser la LPRP de manière à exiger que les institutions fédérales fassent la preuve de la nécessité de la collecte des renseignements personnels avant de les recueillir.

Certaines plaintes sur lesquelles nous avons fait enquête concernaient des questions de longue date touchant la protection de la vie privée, par exemple l'accès des citoyens aux renseignements que détient le gouvernement à leur sujet et le droit des fonctionnaires à la vie privée en milieu de travail.

Nous avons continué de constater des disparités au titre des déclarations d'atteintes à la vie privée dans le secteur public et observé une sous-déclaration systémique, ce qui justifie nos appels répétés en faveur d'une exigence légale de déclaration obligatoire dans le secteur public par le truchement d'une réforme de la LPRP, plutôt que de s'en remettre à une directive du Conseil du Trésor.

En dehors du contexte des enquêtes officielles, nous avons exhorté les institutions fédérales à s'efforcer en priorité de répondre rapidement aux demandes d'accès des Canadiens. Nous avons redoublé d'efforts pour collaborer proactivement avec les fonctionnaires afin de les aider à améliorer leurs pratiques de protection de la vie privée. Dans un contexte où l'on préconise l'adoption des services et technologies numériques, nous avons donné des avis au secteur public fédéral concernant certains programmes et initiatives.

Mises à jour et tendances en matière de fonctionnement

En 2018-2019, le Commissariat a retenu 1 420 plaintes déposées en vertu de la LPRP, comparativement à 1 254 au cours de l'exercice précédent.

Malgré cette hausse, nous avons pu empêcher une nouvelle augmentation de l'arriéré de plaintes déposées en vertu de la LPRP. En outre, nous avons réduit de près d'un mois notre délai de traitement moyen pour les plaintes réglées rapidement.

Les progrès que nous avons réalisés sur ces aspects s'expliquent en partie par la création de la Direction des admissions, du règlement et de la conformité. Cette direction est chargée de la réception et du règlement des plaintes en amont. Elle fait office de filtre pour s'assurer qu'une évaluation approfondie est justifiée dans le cas des plaintes pour lesquelles on demande une enquête officielle.

En outre, la Direction surveille le règlement rapide des plaintes, mécanisme efficace qui donne un résultat satisfaisant pour toutes les parties. Les particuliers y gagnent du fait que l'on répond sans attendre à leurs préoccupations. Les institutions mises en cause en bénéficient aussi, car cela leur évite de consacrer des ressources considérables à un long processus d'enquête plus officiel.

Le Commissariat a systématiquement recours au processus de règlement rapide pour traiter le tiers des plaintes déposées en vertu de la LPRP. Ainsi, sur les 1 366 plaintes en vertu de la LPRP dont le dossier a été clos au cours de l'exercice, 433 ont été réglées rapidement.

Nous nous sommes également attachés à gagner en efficacité après la clôture des enquêtes. Nous avons élargi la portée des fonctions de notre Unité de la surveillance de la conformité de manière à ajouter les plaintes déposées en vertu de la LPRP à celles déposées en vertu de la LPRPDE. Cette unité surveille la mise en œuvre des recommandations formulées à l'issue des enquêtes pour nous donner l'assurance que les institutions respectent les engagements qu'ils ont pris auprès des Canadiens en vertu des lois fédérales sur la protection des renseignements personnels.

Nous nous attendons à ce que cette mesure se traduise par une mise en œuvre plus uniforme des pratiques assurant la protection de la vie privée dans l'ensemble du secteur public.

Nous estimons que le financement temporaire annoncé dans le budget fédéral de 2019 devrait renforcer notre capacité à réduire l'arriéré de plaintes.

Priorité à une réponse rapide aux demandes d'accès déposées par les Canadiens

Malgré notre acharnement à collaborer avec les institutions fédérales en vue de prévenir ou d'atténuer les préoccupations des Canadiens concernant la protection de leur vie privée, il reste des cas où des ministères fédéraux ne traitent pas rapidement les plaintes concernant les réponses tardives aux demandes d'accès déposées en vertu de la LPRP.

Par le passé, nous attendions généralement que le plaignant ait reçu l'information demandée avant de clore nos enquêtes portant sur ces plaintes. Les délais devenaient alors souvent déraisonnables – certaines enquêtes duraient même parfois beaucoup plus longtemps qu'une année.

À l'avenir, le Commissariat s'efforcera de donner plus de pouvoirs aux auteurs des plaintes alléguant que des institutions n'ont pas respecté les délais prévus par la Loi. Dans les cas où nous avons tenté en vain à plusieurs reprises d'amener une institution à répondre rapidement à une demande d'accès ayant fait l'objet d'une plainte, nous considérons que la non-réponse de l'institution constitue un refus d'accès présumé. L'étape suivante consiste à publier un rapport final faisant état de la situation en détail, que le plaignant pourra ensuite déposer à la Cour fédérale.

Au cours de l'exercice écoulé, nous avons constaté 31 cas de refus d'accès présumé mettant en cause trois institutions fédérales, soit Santé Canada, la Gendarmerie royale du Canada (GRC) et le Service correctionnel du Canada (SCC).

Nous préférons encore travailler en collaboration avec les institutions quand elles sont de bonne foi, qu'elles souhaitent collaborer et que les dossiers progressent. Toutefois, lorsque les délais sont déraisonnables, notre priorité est de veiller à ce que les Canadiens puissent exercer leur droit à la vie privée.

Le Commissariat a aussi tenu au printemps 2019 un atelier sur les communications informelles à l'intention du personnel chargé de la protection de la vie privée et du personnel des programmes au sein de différents ministères et organismes fédéraux. Le Commissariat et les participants ont alors pu explorer les défis à relever et les approches novatrices à adopter en ce qui concerne la communication informelle de renseignements personnels en réponse aux demandes reçues d'individus. Le niveau de participation était encourageant.

Les participants à l'atelier ont pu cerner les défis inhérents aux communications informelles :

- les difficultés liées à la décentralisation du traitement des demandes informelles au sein des institutions;
- le manque d'uniformité en matière de formation et de connaissances et les divergences de point de vue du personnel des programmes par rapport à celui des bureaux de l'accès à l'information et de la protection de la vie privée (AIPRP);
- le fait que de nombreux demandeurs préfèrent suivre les canaux officiels pour demander leurs renseignements personnels;
- la gravité des conséquences possibles en cas d'atteinte à la vie privée au cours du traitement des demandes informelles.

L'atelier a donné l'occasion de réfléchir à des solutions pour nombre de ces problèmes. Par exemple, les participants ont notamment discuté de l'idée de mettre sur pied une équipe au sein des bureaux de l'AIPRP pour traiter les demandes informelles ou d'en confier le traitement à une équipe en particulier. Le personnel pourrait bénéficier de processus et de mécanismes bien définis pour les demandes courantes ou fréquentes. Par ailleurs, les institutions pourraient afficher sur leur site Web de l'information expliquant plus clairement aux intéressés où et comment commencer la recherche de leurs renseignements personnels.

Des participants ont suggéré, entre autres, d'avoir recours à des mécanismes de tri pour classer les demandes et déterminer leur ordre de priorité, d'utiliser des technologies nouvelles pour traiter les demandes informelles, et de modifier les processus opérationnels de manière à englober la communication proactive de renseignements.

Nous avons fourni des hyperliens vers les rapports d'enquête ou sommaires de cas pour certaines des enquêtes résumées dans ce rapport annuel. Ces rapports d'enquête ou sommaires de cas sont considérés comme faisant partie intégrante du rapport annuel et sont soumis au Parlement en même temps.

Statistique Canada : Repenser les projets intrusifs de collecte de données en tenant compte du respect de la vie privée

Des enjeux font ressortir l'importance d'entériner dans la loi les critères de nécessité et de proportionnalité

À la fin de l'automne 2018, des médias ont rapporté que Statistique Canada avait recueilli des renseignements détaillés sur le crédit et avait l'intention de recueillir des renseignements détaillés sur les finances de millions de Canadiens auprès d'entreprises du secteur privé – à l'insu des intéressés et sans leur consentement.

Ces reportages ont soulevé une vague d'indignation. Le Commissariat a reçu plus de 100 plaintes d'individus portant sur la collecte de renseignements sur les antécédents en matière de crédit de particuliers et sur la collecte proposée de renseignements sur les transactions financières et sur les soldes de comptes de particuliers auprès de banques.

Les plaignants nous ont dit avoir le sentiment que Statistique Canada ne respectait pas leur droit à la vie privée. Ils ont exprimé des préoccupations concernant ce qui suit : l'autorisation légale de collecte de renseignements conférée à l'organisation; la transparence au sujet des collectes; le traitement des renseignements recueillis, y compris la communication possible – intentionnelle ou non – des renseignements; et le droit d'accès des individus aux renseignements recueillis.

Des renseignements détaillés sur les transactions financières d'un particulier permettent de broser un portrait excessivement précis de son mode de vie,

de ses choix de consommation et de ses intérêts personnels, y compris les choix licites qu'il ne voudrait pas que le gouvernement connaisse. Un dossier complet d'information financière contient donc des renseignements personnels extrêmement sensibles. Dans le même ordre d'idées, des renseignements sur le crédit donnent un très bon aperçu du niveau d'endettement passé et actuel d'un particulier et représentent eux aussi, par leur nature même, des renseignements sensibles.

Les Canadiens étaient préoccupés, à juste titre, des répercussions de ces projets sur leur droit à la vie privée.

Notre enquête n'a pas démontré que Statistique Canada avait enfreint les lois actuelles. Toutefois, elle a permis de soulever des enjeux de vie privée considérables au sujet de ces initiatives.

Cette affaire met également en relief le besoin pressant de réforme législative, pour faire en sorte que la vie privée des Canadiens soit respectée en cette époque où les technologies numériques permettent aux institutions fédérales de recueillir, analyser et stocker de vastes quantités de renseignements personnels.

Les projets en question

Le Commissariat a ouvert une enquête en octobre 2018 au sujet des projets en question, soit le Projet de renseignements sur le crédit et le Projet relatif aux transactions financières.

Les deux projets s'inscrivent dans une initiative de modernisation par laquelle Statistique Canada prévoit utiliser de nouvelles sources publiques et privées de données administratives.

Statistique Canada a fait valoir que les organismes statistiques de partout dans le monde sont aux prises avec une baisse du taux de réponse aux enquêtes, alors que leurs coûts augmentent et que les gouvernements et le secteur privé leur demandent toujours davantage de renseignements statistiques plus à jour et plus détaillés sur la population.

Dans le cadre du Projet de renseignements sur le crédit, Statistique Canada recueillait des données auprès de l'agence d'évaluation du crédit TransUnion, qui lui transmettait des données historiques sur le crédit datant d'aussi loin que 2002, de même que des

renseignements d'identification comme le nom, la date de naissance, le numéro d'assurance sociale et l'adresse. Au bout du compte, TransUnion a transmis à Statistique Canada environ 44 millions de fichiers comprenant des renseignements au sujet de quelque 24 millions de Canadiens. L'écart entre les deux nombres s'explique, en partie, par la présence de fichiers en double pour certains individus et de fichiers de personnes décédées.

Nous avons constaté que Statistique Canada est en mesure de coupler ces données avec d'autres renseignements se trouvant dans ses fonds de données, comme le revenu du ménage et des renseignements sur la propriété recueillis auprès d'autres sources. Bien que Statistique Canada remplace les renseignements d'identification directs par un numéro spécialement créé sur une clé de couplage auquel un nombre très restreint d'employés de l'organisation a accès, il est toujours possible d'identifier les individus à qui appartient l'information au moyen de cette clé de couplage; il est aussi possible que l'information fasse l'objet d'autres couplages que Statistique Canada pourrait effectuer dans l'avenir.

Le Projet relatif aux transactions financières visait à mesurer les dépenses des ménages en recueillant annuellement des renseignements détaillés au sujet des transactions financières et des soldes de comptes de 500 000 particuliers directement auprès d'institutions financières.

Dans le cadre de ce projet, qui n'a pas atteint l'étape de la mise en œuvre, on prévoyait recueillir la date et le montant de toutes les transactions inscrites à un compte personnel pour chaque personne, la description de chaque transaction, le nom du bénéficiaire dans le cas de paiements, et le solde final du compte après la transaction. On aurait également recueilli les identificateurs personnels du titulaire du compte, dont le nom, le numéro d'assurance sociale, la date de naissance, le numéro de téléphone et l'adresse domiciliaire.

Résultats de l'enquête

Nous n'avons pas émis de conclusions au sujet du Projet relatif aux transactions financières, puisqu'aucun renseignement personnel n'a été recueilli.

Néanmoins, nous avons de sérieux doutes quant à la collecte de renseignements dans le cadre du projet tel qu'il était conçu : nous craignons qu'il n'aille au-delà

de l'autorité légale de Statistique Canada en matière de collecte de renseignements personnels, puisque la demande de Statistique Canada aurait exigé la création de nouveaux documents qui n'étaient pas déjà conservés par les institutions financières. De plus, selon ces institutions, cela aurait augmenté les risques pour la sécurité du secteur dans la mesure où ce lot de renseignements sensibles aurait représenté une cible attrayante et de grande valeur pour les pirates informatiques.

En ce qui concerne le Projet de renseignements sur le crédit, nous avons déterminé que Statistique Canada avait l'autorité légale de recueillir les données en question, car ces données se trouvaient dans des documents déjà conservés par TransUnion. Nous avons donc conclu que les plaintes à l'égard de ce projet n'étaient pas fondées.

Cela dit, les deux projets soulevaient des préoccupations sérieuses en matière de vie privée, même si nous sommes d'avis qu'aucun des deux n'a enfreint la loi dans sa forme actuelle. Cette observation met en relief certaines lacunes de la *Loi sur la statistique* et de la LPRP.

Notamment, bien que Statistique Canada ait présenté de nombreux motifs administratifs et stratégiques pour justifier les projets, nous estimons que l'Agence n'a pas démontré que les projets tels qu'ils étaient conçus étaient nécessaires ou proportionnels relativement à leur caractère intrusif.

Nous sommes satisfaits que Statistique Canada ait suspendu ces deux projets à l'automne 2018 et, au terme des discussions dans le cadre de notre enquête, qu'elle ait accepté de mettre en œuvre l'ensemble de nos recommandations, y compris celle de respecter les critères de nécessité et de proportionnalité avant de mettre en œuvre les projets en question.

Nécessité et proportionnalité

Les critères de nécessité et de proportionnalité sont des concepts clés en matière de protection de la vie privée. Il est essentiel pour les institutions fédérales de démontrer que leurs activités et programmes intrusifs sont nécessaires à l'atteinte d'un but précis et légitime, et que leur caractère intrusif est proportionnel au bénéfice attendu.

Même s'il ne s'agit pas d'une exigence de l'état actuel du droit fédéral, la Directive sur les pratiques relatives à la

protection de la vie privée du Secrétariat du Conseil du Trésor du Canada (SCT) exige que les institutions fédérales ne recueillent de renseignements personnels que lorsque cela est « manifestement nécessaire » aux programmes ou aux activités en cours. Il ne suffit pas pour les institutions fédérales de se fier à leur mandat général pour justifier la nécessité d'une entrave à la vie privée.

Le Commissariat recommande depuis plusieurs années que la collecte de renseignements personnels par les institutions fédérales soit régie par une norme de nécessité et de proportionnalité prévue par la loi.

Plusieurs autres autorités législatives, tant au Canada qu'à l'étranger, ont adopté une norme fondée sur la nécessité comme exigence juridique.

Le Canada devrait emboîter le pas et mettre à jour la LPRP pour y inclure cette norme.

Concrètement, nous encourageons les institutions fédérales à soumettre leurs activités et programmes particulièrement intrusifs à une analyse en fonction des questions suivantes :

- La mesure est-elle manifestement nécessaire afin de répondre à un besoin précis?
- L'initiative est-elle susceptible d'être efficace pour répondre à ce besoin?
- La perte de vie privée est-elle proportionnelle au besoin?
- Existe-t-il un moyen moins intrusif d'atteindre la même fin?

Au cours de notre enquête, Statistique Canada a décrit l'objectif public de ces deux projets de manière générale, ce qui est insuffisant pour en démontrer la nécessité.

Toutefois, d'après l'information fournie par l'Agence, nous avons inféré que l'objectif du Projet de renseignements sur le crédit est de fournir des renseignements statistiques fiables à l'appui de politiques visant à pallier les vulnérabilités liées aux finances personnelles des Canadiens, en particulier en ce qui concerne la dette des ménages, les taux d'intérêt et l'évolution du marché immobilier.

Pour ce qui est du Projet relatif aux transactions financières, nous avons inféré que son objectif est de combler des lacunes en matière de données et de produire des renseignements statistiques fiables au

sujet de divers groupes de ménages, afin d'appuyer des politiques économiques et sociales précises, telles que des politiques visant des populations vulnérables et des politiques pour atténuer de manière préventive les conséquences des récessions.

Selon nous, ces objectifs, s'ils sont confirmés par Statistique Canada, pourraient raisonnablement être considérés comme des objectifs publics précis et légitimes. Cela dit, pour déterminer si la collecte des renseignements personnels dans le cadre de ces projets est nécessaire et proportionnelle, il faudrait aussi se demander si l'ensemble des renseignements que l'on prévoit recueillir est manifestement nécessaire et proportionnel à l'atteinte des objectifs. Nous avons conclu que les projets tels qu'ils étaient conçus soulevaient des préoccupations sérieuses quant à savoir si la perte de vie privée était proportionnelle aux besoins en cause.

Au départ, Statistique Canada affirmait que la collecte était « proportionnelle » parce que son objectif était de produire des statistiques agrégées et que l'Agence est tenue de respecter la confidentialité des renseignements personnels.

Nous concédons qu'il s'agit là de facteurs importants, mais ils sont insuffisants dans une analyse de la proportionnalité. Autrement, il n'y aurait pratiquement pas de limite à ce que Statistique Canada pourrait recueillir en vertu de son mandat.

Transparence et sécurité

Nous avons soulevé quelques préoccupations supplémentaires au cours de notre enquête.

Nous avons conclu que Statistique Canada n'a pas démontré un niveau de transparence approprié relativement à la collecte de renseignements personnels prévue dans le cadre des projets en question.

De plus, même si l'Agence a adopté des mesures importantes pour isoler les données, restreindre l'accès à celles-ci et les protéger contre des menaces extérieures, les mesures de sécurité pourraient être améliorées en vue d'atténuer les vulnérabilités internes, par l'entremise d'une surveillance de l'accès et de l'utilisation non autorisés par des usagers internes.

Recommandations

Nous avons émis plusieurs recommandations, que l'Agence s'est engagée à mettre en œuvre :

- ne pas continuer l'exécution du Projet de renseignements sur le crédit tel qu'il avait été conçu à l'origine; par ailleurs, nous encourageons vivement Statistique Canada à éliminer, en temps voulu, les renseignements personnels déjà recueillis qui n'auraient pas été recueillis en vertu du projet reformulé;
- ne pas exécuter le Projet relatif aux transactions financières tel qu'il avait été conçu à l'origine;
- collaborer avec le Commissariat pour reformuler le Projet de renseignements sur le crédit de manière à respecter les principes de nécessité et de proportionnalité;
- collaborer avec le Commissariat pour reformuler le Projet relatif aux transactions financières de manière à respecter l'autorisation légale de l'organisation et les principes de nécessité et de proportionnalité avant d'exécuter ce projet;
- améliorer la transparence concernant la collecte éventuelle de renseignements personnels à partir de sources administratives afin de maintenir la confiance du public;
- mettre en œuvre des mesures pour réduire les risques posés par les vulnérabilités liées aux menaces internes.

En plus de formuler ces recommandations à l'égard de Statistique Canada, nous encourageons le Parlement à envisager une réforme de la *Loi sur la statistique* et de la LPRP afin d'assurer un juste équilibre entre la protection de la vie privée et l'intérêt public au moment d'obtenir des renseignements personnels auprès de sources de données administratives, y compris des entreprises du secteur privé.

La disposition de la *Loi sur la statistique* qui autorise Statistique Canada à accéder à des documents administratifs remonte à 1918, soit bien avant que les organisations commencent à recueillir et à stocker de grandes quantités de renseignements personnels par voie électronique.

En outre, la *Loi sur la statistique* n'oblige pas Statistique Canada à démontrer la nécessité ni la proportionnalité d'une collecte de données administratives renfermant des renseignements personnels. La Loi ne lui impose non plus aucune exigence concernant la minimisation, la transparence et la conservation des données, et ne prévoit pas quand l'organisation peut effectuer des couplages de données pour d'autres études.

Les lacunes de la *Loi sur la statistique* seraient moins préoccupantes si la LPRP n'était pas aussi désuète. La LPRP devrait imposer aux institutions fédérales les exigences de nécessité et de proportionnalité pour la collecte de renseignements personnels.

Prochaines étapes

Nous voyons d'un bon œil que Statistique Canada soit ouverte à l'idée d'adapter ses méthodes pour mieux intégrer les mesures de protection de la vie privée, dont les principes de nécessité et de proportionnalité, dans la conception de nouvelles initiatives statistiques. Nous saluons son engagement à cet égard et sommes d'avis qu'il s'agit là d'un pas important pour renforcer la confiance du public.

Nous espérons que l'expérience de Statistique Canada servira de modèle à d'autres institutions fédérales alors qu'elles sont en voie d'arrimer leurs activités à la Feuille de route de la Stratégie de données pour la fonction publique fédérale.

Rapport de conclusions

Enquête portant sur Statistique Canada



Autres enquêtes majeures

Une enquête met en lumière de sérieuses lacunes dans la fouille d'appareils numériques à la frontière

La fouille des appareils numériques personnels – en particulier les téléphones cellulaires, les tablettes électroniques et les ordinateurs portables – par les agents des services frontaliers du Canada a donné lieu à plusieurs plaintes contre l'Agence des services frontaliers du Canada (ASFC).

Les appareils numériques permettent de stocker une grande quantité de renseignements très confidentiels et très personnels. Lorsqu'ils sont connectés à Internet, ces appareils donnent accès à des renseignements personnels qui ne se limitent pas à ceux se trouvant généralement dans les bagages d'un voyageur – loin de là. La fouille des appareils numériques met donc en jeu d'importants aspects du droit à la vie privée.

Au cours de notre enquête, nous avons découvert que le contenu examiné par les agents dans ces dossiers comprenait notamment des documents, des textos, des photographies, des messages dans Facebook et WhatsApp, l'historique des sites Web consultés et des renseignements bancaires en ligne.

Les plaignants, qui étaient tous des citoyens canadiens de retour au pays après un voyage à l'étranger, remettaient en question le pouvoir de l'Agence d'effectuer ce type de fouilles.

La *Loi sur les douanes* autorise les agents des services frontaliers à examiner, à des fins liées à l'administration des douanes, toute « marchandise » qui est « importée » au Canada pour assurer la conformité aux lois administrées ou appliquées par l'ASFC. Par définition, les « marchandises » englobent « tout document, quel que soit son support ». L'Agence a soutenu que les documents électroniques stockés sur les appareils numériques sont couverts par cette définition.

L'ASFC reconnaît que son pouvoir ne lui permet pas d'examiner les documents électroniques qui ne sont pas stockés sur un appareil numérique, mais auxquels on peut avoir accès à partir d'un appareil en se connectant à Internet.

Afin de s'assurer que les agents des services frontaliers consultent uniquement les renseignements stockés sur les appareils, l'ASFC a adopté une politique interne exigeant que la connectivité réseau des appareils compatibles avec Internet soit désactivée avant une fouille.

Toujours selon la politique de l'ASFC, la fouille des appareils numériques ne devrait pas être systématique. Cette politique autorise les agents des services frontaliers à effectuer un examen progressif des appareils numériques en présence de plusieurs indicateurs d'une éventuelle infraction ou par suite de la découverte de marchandises non déclarées, faussement déclarées ou interdites. En outre, en vertu de la politique, l'agent doit consigner les types de données examinées et les motifs à l'origine de cet examen.

L'enquête a mis en lumière plusieurs manquements des agents des services frontaliers concernant la conformité à la politique interne de l'ASFC et aux exigences de la *Loi sur les douanes*.

Par exemple, dans un cas, un agent a utilisé l'appareil d'une plaignante pour avoir accès à des renseignements bancaires en ligne, soit des renseignements qui n'étaient pas stockés sur l'appareil et accessibles uniquement par Internet.

En outre, comme l'a reconnu l'ASFC, dans quatre des six cas, le mode avion de l'appareil n'avait pas été activé, contrairement à la politique de l'Agence. Dans les deux autres cas, les agents n'avaient inscrit aucune note indiquant si ce mode avait été activé.

Nous avons également découvert d'autres manquements. Dans un des cas, un agent a photographié le contenu du téléphone cellulaire du plaignant comme preuve d'une infraction possible au *Code criminel* – mesure que ne permet ni le pouvoir de faire des copies de documents prévu dans la *Loi sur les douanes* ni celui de saisir des éléments de preuve en vertu du *Code criminel*.

En outre, dans les six cas examinés, les agents des services frontaliers n'avaient consigné ni les indicateurs ayant conduit à la fouille des appareils, ni les emplacements des appareils numériques consultés, ni les raisons pour lesquelles il y avait eu fouille dans ces emplacements.

Les nombreux manquements que nous avons soulevés nous portent à croire à un manque de formation, de sensibilisation et de reddition de comptes pour s'assurer que les agents des services frontaliers se conforment aux exigences de la *Loi sur les douanes*, de la LPRP et de la politique de l'ASFC. Par conséquent, le droit à la vie privée des Canadiens n'est pas respecté au cours de la fouille des appareils aux postes frontaliers.

Les manquements relevés dans les pratiques de l'ASFC révèlent des problèmes chroniques qui touchent directement la responsabilité de l'Agence auprès du public, tant pour l'exercice des pouvoirs qui lui sont conférés que pour le respect des exigences de la *Loi sur la protection des renseignements personnels*.

Le Commissariat a formulé à l'intention de l'ASFC plusieurs recommandations afin qu'elle corrige les manquements que nous avons observés, dont les suivantes :

- Mettre en œuvre un programme de formation obligatoire pour tous les agents – nouveaux ou en poste – et leurs superviseurs afin qu'ils soient correctement formés pour effectuer des examens progressifs des appareils et des supports numériques. Documenter la participation du personnel à ce programme.
- Mettre en place des mécanismes de surveillance et d'examen pour vérifier la conformité des agents des services frontaliers à la politique et aux pratiques de l'ASFC concernant l'examen des appareils numériques, comme les inspections par les agents, la vérification des cahiers de notes ou des systèmes, et les indicateurs d'examen d'appareils numériques dans les systèmes.
- Réaliser une vérification indépendante de l'application de sa politique et du cadre opérationnel pour l'examen des appareils numériques en vertu de la *Loi sur les douanes*.
- Mettre à jour le Manuel de l'exécution de manière à tenir compte des exigences de la politique actuelle de l'ASFC.

- Publier sur son site Web la politique, ainsi que tout autre guide et bulletin opérationnel pertinent, de manière à accroître la transparence et le principe de responsabilité.
- Compiler et produire des données statistiques se rapportant à son examen des appareils numériques et rendre ces renseignements accessibles au public de manière proactive.

L'ASFC a accepté les recommandations formulées par le Commissariat. Par conséquent, le Commissariat considère les six plaintes fondées et conditionnellement résolues.

Outre ces recommandations, le Commissariat exhorte le Parlement à modifier la *Loi sur les douanes* afin de mieux protéger le droit à la vie privée des voyageurs à la frontière, et a correspondu à cet effet avec le ministre de la Sécurité publique et de la Protection civile et avec le ministre de la Sécurité frontalière et de la Réduction du crime organisé.

Plus précisément, nous estimons qu'il faudrait mettre à jour la *Loi sur les douanes* afin de reconnaître que les appareils numériques renferment des renseignements personnels sensibles et qu'il ne s'agit donc pas de simples « marchandises » au sens de la *Loi sur les douanes*. En outre, cette loi devrait inclure un cadre législatif clair quant à l'examen des appareils numériques. Il faudrait aussi rehausser le seuil pour l'examen des appareils numériques de sorte que les agents devraient avoir des « motifs raisonnables de soupçonner » une infraction à la loi.

Rapport de conclusions

Enquête portant sur l'ASFC



Affaires mondiales Canada demande des détails sur les voyages personnels d'un employé figurant sur son passeport diplomatique

Un employé d'Affaires mondiales Canada (AMC) en mission à l'étranger qui détenait un passeport diplomatique du gouvernement du Canada s'était servi de ce passeport à l'occasion pour des voyages personnels. Le passeport diplomatique contenait donc des renseignements sur ces voyages (p. ex., visas, timbres des postes frontaliers et dates des déplacements).

AMC a demandé à l'employé de lui rendre son passeport diplomatique comme preuve dans le cadre d'une enquête administrative. Lorsque l'employé a présenté une photocopie des pages de son passeport diplomatique montrant ses voyages professionnels, AMC a insisté pour qu'il rende le passeport original. Le plaignant a refusé, alléguant que le Ministère demandait à certains employés d'utiliser leur passeport diplomatique pour leurs voyages personnels.

AMC a soutenu que le passeport diplomatique est la propriété du gouvernement du Canada et qu'il peut être repris en tout temps. Le Ministère a affirmé avoir, dans le dossier, le pouvoir de recueillir les renseignements sur les voyages personnels du plaignant en lien avec des allégations d'inconduite. AMC n'a fourni aucune information sur la nature de l'enquête administrative en question.

Le passeport diplomatique indique le nom du titulaire, sa date de naissance et sa citoyenneté, ainsi que ses antécédents de voyages personnels. Or, selon la *Loi sur la protection des renseignements personnels*, « [I]es seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités ».

AMC n'a pas réussi à faire la preuve au Commissariat que les antécédents de voyages personnels du plaignant étaient pertinents pour l'enquête ni qu'ils en faisaient l'objet. En fin de compte, les renseignements personnels du plaignant n'ont pas été recueillis, car celui-ci n'a pas rendu son passeport diplomatique comme demandé. Le Commissariat a toutefois conclu que la plainte était fondée.

Ce cas pourrait revêtir un caractère systémique et avoir une incidence sur d'autres personnes utilisant un passeport diplomatique. Nous avons donc recommandé à AMC de préciser les dispositions de sa politique et

de ses pratiques concernant l'utilisation personnelle des passeports diplomatiques et leur incidence sur la protection de la vie privée. Nous lui avons également recommandé de communiquer cette information à toute personne pouvant être appelée à utiliser un passeport diplomatique à des fins personnelles. Par exemple, AMC pourrait informer les titulaires d'un passeport diplomatique des situations où le Ministère est habilité à recueillir des renseignements de voyages personnels et leur indiquer, par la même occasion, les utilisations autorisées énoncées dans les instructions ministérielles. AMC était en désaccord avec nos recommandations, mais a accepté d'examiner l'information communiquée aux titulaires d'un passeport diplomatique concernant la collecte et l'utilisation de leurs renseignements personnels.

Rapport de conclusions

Enquête portant sur AMC



Des renseignements inexacts donnent lieu à une embauche par inadvertance et à des problèmes de paye pour un fonctionnaire

Une erreur sur la personne s'est avérée exaspérante et coûteuse pour un employé de Services publics et Approvisionnement Canada (SPAC) qui a été embauché par inadvertance à un poste pour lequel il n'avait pas présenté sa candidature à ISDE.

La confusion est attribuable à un logiciel de gestion des ressources humaines – MesRHGC – qui automatise les fonctions relatives aux ressources humaines, par exemple la dotation, la classification, les horaires et les congés. SPAC est chargé de la mise en œuvre, de l'hébergement et de la maintenance du logiciel. Ce ministère offre également de la formation aux institutions fédérales qui l'utilisent.

Lorsqu'un ministère souhaite embaucher une personne, il vérifie si elle a un profil dans MesRHGC. Le cas échéant, la personne est sélectionnée et son profil est transmis au ministère d'embauche.

Au moment de l'incident, les responsables des ressources humaines à ISDE avaient eu pour instructions de faire une recherche dans MesRHGC en utilisant

le prénom et le nom d'une personne. On ne leur avait pas demandé d'utiliser systématiquement un troisième champ de données, comme le code d'identification de dossier personnel (CIDP) ou la date de naissance.

Le problème dans ce dossier découle du fait que le plaignant – dont le nom est identique à celui du candidat retenu – avait été sélectionné dans le système sans même avoir posé sa candidature au poste offert. À cause de l'erreur, l'employé a été considéré dans MesRHGC comme ayant « quitté » son poste à SPAC et n'a pas été rémunéré pour certaines périodes de paye en attendant que le problème soit résolu.

Le plaignant alléguait qu'ISDE avait enfreint les dispositions de la LPRP régissant l'exactitude des renseignements en utilisant des renseignements inexacts à son sujet pour doter un poste. Afin d'éviter qu'une erreur similaire ne se reproduise, ISDE a créé un document pour indiquer aux employés qu'ils doivent valider l'identité des personnes au moyen de champs de données comme le CIDP ou la date de naissance.

Comme ISDE n'est pas chargé d'apporter des changements à MesRHGC, nous estimons qu'il a pris des mesures raisonnables pour assurer l'exactitude des renseignements qu'il utilise pour sélectionner des profils dans MesRHGC. Toutefois, MesRHGC est largement utilisé dans l'ensemble du gouvernement et permet encore de sélectionner des personnes uniquement à partir de leur prénom et de leur nom, sans avoir à remplir d'autres champs de données.

L'Office des transports du Canada refuse à un défenseur des droits des passagers aériens l'accès à ses renseignements personnels

Un défenseur des droits des passagers aériens a déposé une plainte dans laquelle il accusait l'Office des transports du Canada (OTC) d'invoquer à tort des exceptions en matière de communication pour lui refuser l'accès aux renseignements personnels le concernant.

L'OTC avait donné au plaignant accès à 33 pages complètes ou partielles de documents, mais lui avait refusé l'accès à 760 pages complètes en invoquant des dispositions de la LPRP. Dans bien des cas, les renseignements non communiqués comprenaient des points de vue sur le comportement du plaignant ou d'autres renseignements le concernant, entre autres la façon dont l'Office a traité ses demandes et les renseignements que l'Office a recueillis à son sujet à partir d'articles de journaux. Il s'agissait principalement de communications entre des employés de l'OTC, et non de notes prises par des décideurs susceptibles de faire l'objet d'un privilège décisionnel.

Cependant, on a dit au plaignant que la plupart des renseignements ne correspondaient pas à la définition de « renseignements personnels » au sens de la Loi, puisqu'il agissait en qualité de représentant d'un groupe de défense des droits des consommateurs et non à titre personnel. L'OTC a fait valoir que le nom du plaignant ne devait pas être considéré comme un renseignement personnel lorsqu'il s'agit d'une question d'ordre réglementaire ou décisionnel portée à son attention par le plaignant au nom d'une organisation.

Le plaignant a répondu que le groupe de défense des droits qu'il représente n'est pas constitué en personne morale distincte. Il a précisé que toutes les plaintes qu'il avait déposées contre l'OTC l'avaient été en son nom personnel, tout comme les poursuites découlant de ces plaintes.

Le Commissariat a conclu que l'OTC s'appuyait sur une interprétation erronée de la définition de « renseignements personnels » énoncée dans la Loi afin de ne pas communiquer des renseignements au plaignant et que la plainte était fondée. Il a donc recommandé à l'Office de donner au plaignant accès à ses renseignements personnels dont la communication lui avait été refusée sous réserve des autres exceptions applicables, par exemple le secret professionnel de l'avocat.

Rapport de conclusions

Enquête portant sur ISDE

Le Commissariat a accordé à l'OTC jusqu'au 1^{er} mars 2019 pour donner au plaignant une réponse complète. L'Office n'a pu respecter cette échéance, mais il a indiqué au Commissariat qu'il avait communiqué les renseignements personnels au plaignant le 18 mars 2019. Le plaignant a exercé un recours en révision devant la Cour fédérale en vertu de l'article 41 de la Loi au sujet de la réponse de l'OTC à sa demande d'accès. Au moment de rédiger ce rapport, l'affaire était devant la Cour.

Rapport de conclusions

Enquête portant sur l'OTC

Utilisation, par Emploi et Développement social Canada, d'une liste d'un courtier en données pour envoyer des courriels non sollicités

Une plainte déposée contre Grey House Publishing Canada en vertu de la LPRPDE a aussi abouti au dépôt d'une plainte contre Emploi et Développement social Canada (EDSC). Ces plaintes montrent un exemple intéressant du point de convergence entre les dispositions de la LPRP et celles de la LPRPDE concernant la collecte et l'utilisation des mêmes renseignements.

Le plaignant alléguait que Grey House avait recueilli, utilisé et communiqué ses renseignements personnels en vertu d'une entente de service conclue avec EDSC. Grey House devait fournir au Ministère une liste de distribution renfermant plus de 40 000 adresses de courriel, dont certaines se rapportaient à des associations et à des organismes à but non lucratif. Le nom du plaignant, son adresse de courriel et son numéro de téléphone – que Grey House avait obtenus dans un site Web où le plaignant figurait à titre de personne-ressource pour la section ou le « cercle » local d'une association nationale à but non lucratif – avaient été transmis à EDSC.

Le Ministère a utilisé la liste fournie par Grey House afin d'envoyer au plaignant des courriels non sollicités faisant la promotion du Prix du Premier ministre pour le bénévolat, programme qu'il administre. Selon le plaignant, Grey House aurait recueilli et communiqué ces renseignements à son insu et sans son consentement. Malgré l'absence de consentement, le courriel envoyé par EDSC indiquait à tort que les destinataires du message figuraient sur une liste d'abonnés appartenant à Grey House Publishing Canada. Le plaignant avait aussi demandé l'année précédente à EDSC de retirer son nom de sa liste d'envoi, mais le Ministère n'avait pas donné suite à sa demande et n'en avait pas informé Grey House.

Nous avons remarqué que, en vertu du contrat conclu avec EDSC, Grey House devait recueillir les coordonnées en conformité avec la législation canadienne et obtenir tous les consentements nécessaires. Dans ce dossier, l'entreprise avait recueilli les coordonnées du plaignant à son insu et sans son consentement, ce qui contrevient à la LPRPDE et aux modalités du contrat. Comme il incombait à EDSC de s'assurer que Grey House se conformait aux modalités du contrat, la collecte des coordonnées du plaignant ne correspondait pas aux paramètres définis par le Ministère pour le programme. En conséquence, nous avons conclu que leur collecte contrevenait à l'article 4 de la LPRP.

Depuis, le nom du plaignant a été retiré de la liste de distribution par courriel d'EDSC et le plaignant n'a reçu aucun autre courriel du Ministère concernant les prix. De plus, EDSC a apporté des modifications à ses processus afin d'éviter que le problème se reproduise.

Documents connexes

Rapport de l'enquête portant sur EDSC

Résumé des conclusions de l'enquête portant sur Grey House

Exemple de réussite du règlement rapide

Un individu a demandé à une institution fédérale de lui donner accès à ses renseignements personnels. L'institution lui a répondu qu'elle n'avait pas l'information demandée. Insatisfait de la réponse, cet individu a déposé une plainte auprès du Commissariat. Un enquêteur du Commissariat a alors contacté l'institution, qui lui a confirmé qu'elle ne détenait pas l'information en question. Après avoir fait quelques appels téléphoniques, notre enquêteur a pu déterminer quelle institution était en possession de l'information et obtenir la confirmation que celle-ci donnerait suite à la demande du plaignant. L'enquêteur a communiqué cette information au plaignant, qui a alors pu présenter à l'institution visée une nouvelle demande d'accès à ses renseignements personnels.

Ce dossier fait ressortir l'intérêt du règlement rapide des plaintes par rapport aux longues enquêtes. Dans la mesure du possible, le Commissariat privilégie le traitement des problèmes de protection de la vie privée dès le début et la résolution des problèmes en collaboration, en dehors du processus officiel d'application de la loi.

Mise à jour sur les déclarations d'atteintes à la vie privée

Le nombre de déclarations d'atteintes à la vie privée émanant des institutions publiques a chuté de 46 % en 2018-2019. Le Commissariat n'a reçu que 155 déclarations émanant du secteur public, soit beaucoup moins que les 286 déclarations de 2017-2018.

De fait, le nombre de déclarations d'atteintes à la vie privée a beaucoup fluctué depuis mai 2014, date d'entrée en vigueur d'une directive du Conseil du Trésor obligeant les institutions fédérales à déclarer au Commissariat les atteintes « substantielles » à la vie privée.

Tout porte à croire qu'il y a une sous-déclaration systémique de certains types d'atteintes à la vie privée dans l'ensemble du gouvernement. La grande majorité (84 %) des déclarations d'atteintes à la vie privée reçues par le Commissariat se rapportent à des renseignements communiqués par accident ou perdus. Rien n'indique que le secteur public est à l'abri des cyberatteintes, mais seulement quelques atteintes de cette nature nous ont été déclarées à ce jour par les institutions du secteur public. Par ailleurs, nous n'avons reçu en 2018-2019 que 17 déclarations d'atteintes se rapportant à un accès non autorisé à des renseignements personnels.

Notre examen des déclarations d'atteintes à la vie privée émanant des institutions fédérales au cours de l'exercice précédent avait soulevé plusieurs préoccupations concernant la déclaration de ces atteintes dans le secteur public, notamment des questions concernant la responsabilité en matière de protection de la vie privée, les mesures de protection visant les technologies de l'information et les connaissances des travailleurs de première ligne quant à la nature même des renseignements personnels.

Par exemple, nous avons observé une certaine confusion sur la question de savoir si un passeport canadien représente un renseignement personnel sensible. C'est pourquoi nous avons lancé une vérification à petite échelle portant sur les pratiques de gestion des passeports par le gouvernement.

Bon nombre des institutions visées par notre examen ont reconnu que leurs employés ne comprennent pas pleinement en quoi consistent les renseignements personnels et quelles sont les obligations leur incombant en vertu de la Loi.

En guise de suivi des conclusions de notre étude sur les déclarations d'atteintes à la vie privée dans une optique plus générale, nous avons exhorté le SCT à renforcer son offre d'orientation et d'outils stratégiques, ainsi qu'à améliorer la sensibilisation et la formation au sein des institutions fédérales. Pour ce faire, le SCT a élaboré un plan d'action et nous tient au courant de ses avancées. Le SCT nous a rapporté entre autres avoir intensifié ses activités d'engagement avec les intervenants, avoir pris part à des rencontres avec des communautés de pratique clés, et être en voie d'élaborer du matériel de formation et des outils à l'intention des fonctionnaires fédéraux. Au moment de la rédaction du présent rapport, nous continuons de suivre les progrès et attendons l'occasion d'examiner des documents et outils concrets.

Nous travaillons actuellement avec le SCT à la création d'un formulaire de déclaration des atteintes en ligne qui aidera les institutions à fournir une information plus complète. Le SCT offrira également de l'orientation sur les exigences en matière de déclaration des atteintes.

Nous recommandons depuis nombre d'années de modifier la LPRP de manière à rendre obligatoire la déclaration des atteintes à la vie privée. D'après nous, il faudrait obliger explicitement les institutions fédérales à déclarer rapidement au Commissariat les atteintes à la sécurité des renseignements personnels et à aviser les personnes touchées, s'il y a lieu.

Nous constatons de nombreux manques d'uniformité dans l'application de la directive du Conseil du Trésor par les institutions fédérales. L'adoption de dispositions législatives obligeant ces institutions à déclarer au Commissariat les atteintes à la vie privée nous donnerait l'assurance d'avoir une meilleure idée de l'ampleur actuelle du problème. Elles nous donneraient également l'assurance que nous serions consultés au moment d'élaborer les mesures à prendre pour réagir aux atteintes et atténuer leurs répercussions sur les individus. Ce changement résoudrait également le problème du décalage entre les lois sur la protection des renseignements applicables au secteur public fédéral et au secteur privé canadiens.

Le Commissariat utilise les déclarations d'atteintes à la vie privée qu'il reçoit du secteur public pour s'assurer que les intérêts des Canadiens sont dûment pris en compte et pour aider les institutions fédérales à atténuer les préjudices qu'ils subissent. Ces déclarations sont

indispensables pour aider le Commissariat à évaluer les pratiques de gestion des atteintes en général et déterminer quand et comment réduire les risques d'atteinte à la vie privée en formulant des avis et en recommandant des mesures. C'est pourquoi il est essentiel que les atteintes soient déclarées au Commissariat comme il se doit.

Conseils aux institutions fédérales

La Direction des services-conseils au gouvernement vient de terminer sa première année d'existence. Elle formule des avis et des recommandations à l'intention des institutions fédérales au sujet d'initiatives et de programmes particuliers. Elle examine également les EFVP et les ententes de communication d'information présentées par les ministères et organismes.

Cette direction mène aussi diverses initiatives de sensibilisation auprès du secteur public fédéral afin d'encourager la conformité à la LPRP. L'objectif visé est d'informer les ministères et de leur donner des avis au moment où ils conçoivent ou modifient leurs services de manière à réduire le plus possible le risque d'atteinte à la sécurité des renseignements personnels des Canadiens, notamment au moment de la conception de programmes nouveaux et novateurs. Les avis formulés par la Direction ont pour but d'aider les institutions à atténuer les répercussions sur la vie privée avant la mise en œuvre des programmes.

Dans la mesure du possible, le Commissariat privilégie le traitement des problèmes de protection de la vie privée dès le début de manière proactive et collaborative, en dehors du processus officiel d'application de la Loi. Cette approche offre aux institutions fédérales une certaine uniformité et une certaine prévisibilité dans leurs rapports avec le Commissariat et contribue à faire en sorte que les avantages de l'innovation technologique l'emportent sur les risques.

Le Commissariat donne aux institutions fédérales des avis informels et examine les EFVP depuis nombre d'années; néanmoins, la Direction des services-conseils au gouvernement a été créée en temps opportun. Le gouvernement du Canada s'est engagé à avoir davantage recours aux services numériques et à tirer parti de moyens novateurs d'utiliser et d'échanger les données, de manière à fournir des programmes et des services aux Canadiens de façon plus efficiente.

Comme on pouvait s'y attendre, le nombre de demandes de consultations proactives reçues d'institutions fédérales a doublé au cours de la première année d'existence de la Direction.

Recommandations du Commissariat sur les initiatives de gouvernement numérique

- Une autorisation législative s'impose pour recueillir et communiquer les renseignements personnels. La responsabilité pour la gestion des renseignements personnels doit être définie clairement et bien documentée.
- Les institutions devraient recueillir uniquement les renseignements nécessaires à la mise en œuvre d'un programme ou d'un service.
- Les mesures de protection comme les mesures de contrôle d'accès et de prévention des atteintes devraient être intégrées dès le début et en place avant la mise en œuvre.
- Le rôle et les responsabilités des fonctionnaires en matière de protection de la vie privée devraient être clairement documentés et bien compris.
- Les institutions fédérales devraient faire preuve de transparence concernant la façon dont elles recueillent, utilisent et communiquent les renseignements personnels, notamment la manière dont elles peuvent les combiner, les coupler, les analyser et les évaluer pour créer de nouveaux éléments d'information.
- Le Commissariat devrait être consulté dès le début du processus d'élaboration afin de pouvoir donner un avis utile en matière de protection de la vie privée avant la mise en œuvre de nouveaux programmes ou activités.

En 2018-2019, la Direction des services-conseils au gouvernement a formulé des avis sur diverses initiatives et innovations en matière de gouvernement numérique. Elle a consulté les institutions fédérales sur l'élaboration et l'utilisation des analyses avancées et prédictives, qui vont en augmentant au sein du gouvernement dans son ensemble.

Nous avons aussi émis un avis sur les programmes d'authentification et de vérification de l'identité, notamment l'approche « une fois suffit » et la mise en œuvre prévue d'une seule identité numérique fiable permettant aux individus d'avoir accès à plusieurs services et comptes du gouvernement. Nous avons également donné un avis sur l'élargissement de la portée des demandes en ligne pour les services en matière d'immigration, les services sociaux, les impôts et les régimes de retraite.

Nous avons consulté l'Agence du revenu du Canada (ARC), EDSC et le SCT sur un programme permettant aux individus d'avoir accès en ligne à la fois au service Mon dossier de l'ARC et à Mon dossier Service Canada d'EDSC en s'inscrivant à l'un des deux. Les utilisateurs pourraient utiliser les mêmes données de connexion afin de voir l'information et d'apporter des modifications au cours d'une seule session.

Le Commissariat a également engagé un dialogue avec l'ARC et EDSC concernant l'Initiative d'échange de renseignements sur l'adresse et le dépôt direct. Grâce à cette initiative, les prestataires du Régime de pensions du Canada traitent avec un seul ministère pour communiquer ou mettre à jour leurs renseignements pour le dépôt direct. Par la suite, les deux organisations communiquent et utilisent ces renseignements pour tous les programmes de prestations et de crédits d'impôt que l'une ou l'autre administre.

En outre, nous avons exprimé un avis sur diverses utilisations novatrices de la technologie ainsi que sur la collecte et l'analyse de données à l'échelle du gouvernement, par exemple les initiatives présentées ci-après.

Plateforme de dotation Nuage de talents du SCT

Le SCT dirige l'initiative de la plateforme de dotation Nuage de talents pour les institutions fédérales cherchant à embaucher des employés pour une période déterminée dans le cadre de projets. Le SCT a déposé au Commissariat une EFVP portant sur la première étape du projet Nuage de talents.

À l'issue de l'examen de cette EFVP, nous avons déploré que les candidats à un emploi aient l'option de fournir des renseignements biographiques dans des champs de texte libre. Cette pratique crée un risque de collecte excessive de renseignements personnels, notamment des renseignements sensibles.

Nous avons également recommandé au SCT de communiquer de manière sécurisée les renseignements personnels des candidats aux ministères recruteurs en vertu d'ententes de communication d'information établissant clairement les modalités de cette communication. Le SCT a bien accueilli nos recommandations et indiqué qu'il tiendrait compte de nos commentaires pour la suite de l'initiative. Le Nuage de talents est en phase pilote. Les prochaines étapes comprendront un portail pour les talents autochtones, un modèle d'embauche faisant appel à des outils d'atténuation des préjugés et la vérification en ligne des titres de compétence des candidats au moyen de la technologie des chaînes de blocs. Le SCT a l'intention de présenter deux EFVP supplémentaires concernant les étapes prévues.

Initiative Ressources humaines et paye de la prochaine génération du SCT

Le SCT pilote l'initiative Ressources humaines et paye de la prochaine génération, qui explore une solution en matière de ressources humaines et de rémunération des employés pour la fonction publique fédérale et qui assure la stabilisation du système de paye Phénix. Le Commissariat travaille en consultation avec le SCT et formule des avis concernant les exigences relatives à la protection de la vie privée associées aux solutions proposées.

Au cours des consultations préliminaires sur les solutions possibles, nous avons exprimé notre préoccupation quant à l'utilisation de renseignements permettant d'identifier des individus à l'étape des essais avant et pendant les projets pilotes. Nous avons recommandé au SCT de retirer les identifiants ou de conclure de solides ententes de communication d'information avec les fournisseurs pour s'assurer que les renseignements ont été anonymisés. Le SCT nous a donné l'assurance que les renseignements ne renfermeraient aucun identificateur personnel et qu'il conclurait des ententes de confidentialité avec les

fournisseurs éventuels. Nous nous attendons à recevoir une EFVP pour un ou plusieurs projets pilotes liés à cette initiative.

Projet de surveillance des médias sociaux *Wide Awake* de la GRC

Le projet *Wide Awake* de la GRC fait appel à des outils qui analysent le contenu affiché dans les médias sociaux. Le but est de détecter proactivement les menaces à la sécurité publique afin que la GRC puisse intervenir en cas de besoin. Les représentants du Commissariat ont rencontré ceux de la GRC dès le début de la conception de cet outil. Le Commissariat a recommandé que le projet fasse l'objet d'une EFVP. En réponse aux préoccupations exprimées par le Commissariat en ce qui a trait à la transparence, la GRC lui a fait part de son intention d'afficher sur son site Web un résumé de sa politique en matière d'analyse des médias sociaux. Elle a fait remarquer que les policiers ont uniquement accès à l'information accessible au public dans les médias sociaux. Comme nous l'avons souligné, bien que l'attente en matière de protection de la vie privée soit moindre dans le cas de l'information à laquelle le public a accès, il reste à cet égard une attente raisonnable qui requiert une protection.

Renseignements sur les voyageurs de l'ASFC

Nous avons reçu de nombreuses EFVP à portée restreinte concernant l'utilisation des renseignements sur les voyageurs. Nous avons donc demandé à l'ASFC de nous fournir une vue d'ensemble des risques d'atteinte à la vie privée associés à la collecte, à l'utilisation, à l'analyse et à la communication des renseignements sur les passagers aériens effectués dans le cadre du Programme d'information préalable sur les voyageurs et du dossier passager (IPV/DP). Ce programme prévoit la collecte de renseignements prescrits auprès des transporteurs aériens commerciaux pour détecter les personnes qui participent ou pourraient participer à des activités terroristes, à des crimes liés au terrorisme ou à d'autres crimes graves, y compris le crime organisé, de nature transnationale.

L'Agence a présenté une EFVP générale portant sur l'acquisition de ces renseignements ainsi qu'une série d'EFVP supplémentaires sur leurs utilisations ultérieures.

Ces EFVP comprennent une description des premières acquisitions de renseignements, de l'analyse de ces renseignements, du ciblage des passagers aériens ainsi que du développement de produits de renseignement et de la communication d'information générée par les renseignements, notamment sous l'égide du Programme de ciblage fondé sur des scénarios, que [le Commissariat a examiné en 2017](#).

Nous avons précédemment discuté avec l'ASFC de la nécessité et de la proportionnalité de ce programme. Nous avons également exprimé nos préoccupations concernant les scénarios de risques élaborés à partir de caractéristiques personnelles recueillies dans l'IPV/DP, comme l'âge, le sexe, l'origine du document de voyage, l'itinéraire, le temps passé à l'étranger et l'historique des voyages. Ces éléments d'information servent à analyser les renseignements sur les voyageurs et à cibler les personnes susceptibles de justifier un renforcement de la sécurité au moment de leur arrivée au Canada.

À l'issue de l'examen du Programme de ciblage fondé sur des scénarios mené en 2017, nous avons recommandé d'examiner les scénarios du point de vue des répercussions sur la vie privée, des droits de la personne et des libertés civiles avant leur lancement et sur une base régulière. Nous avons précisé que les décisions prises concernant la modification ou la suppression de certains scénarios à la suite de ces examens devraient être clairement documentées. De plus, nous avons recommandé de modifier ou d'éliminer les scénarios qui ne respectent pas les critères d'efficacité.

D'après l'EFVP du Programme IPV/DP de l'ASFC, l'organisme a mis à jour son cadre de gouvernance pour l'évaluation des scénarios utilisés dans le ciblage fondé sur des scénarios en mars 2018. Dans l'EFVP, l'Agence affirme avoir pris cette mesure en réponse à notre examen d'une EFVP en 2017, qui recommandait l'adoption d'un processus d'évaluation documenté afin de mesurer les répercussions éventuelles sur la vie privée, les libertés civiles et les droits de la personne.

Pendant l'examen du Programme de ciblage fondé sur des scénarios mené en 2017, nous avons également exprimé nos préoccupations à l'idée que les renseignements personnels d'individus ciblés par le Programme IPV/DP et jugés non menaçants pourraient être communiqués à des partenaires nationaux et

étrangers au début du processus d'examen. Il y a donc un risque que ces renseignements soient conservés inutilement ou communiqués par la suite. Nous avons recommandé à l'ASFC d'examiner les ententes de communication d'information conclues avec ses partenaires en portant attention à ce risque. L'ASFC a accepté d'examiner à l'interne les principales ententes de communication d'information. D'ailleurs, l'EFVP qu'elle nous a présentée en 2018 fait état de cet examen. Nous continuons de travailler en consultation avec l'ASFC sur ce programme.

Alertes du commissaire à la protection de la vie privée

Les [Alertes du commissaire à la protection de la vie privée](#) ont été lancées en 2018-2019. Cette nouvelle initiative permet au Commissariat de faire connaître à l'ensemble de la fonction publique les nouvelles, les tendances et les renseignements importants en matière de protection de la vie privée ainsi que les leçons apprises et les pratiques exemplaires observées en collaborant avec les coordonnateurs de l'accès à l'information et de la protection des renseignements personnels. Ces alertes sont transmises par courriel à mesure que les enjeux et les tendances se profilent.

Au moment de rédiger ce rapport, des alertes avaient été émises sur l'utilisation de dispositifs de stockage portables, la sous-traitance de fonctions à un tiers, ainsi que l'importance de saines pratiques de conservation des données pour réduire l'impact d'éventuelles atteintes à la vie privée.

Nous savons qu'il y a de nombreuses leçons à tirer de nos enquêtes, des atteintes à la vie privée déclarées au Commissariat, de notre examen des évaluations des facteurs relatifs à la vie privée et des services-conseils que nous offrons aux institutions fédérales. En raison des dispositions de la LPRP concernant la confidentialité, il est parfois difficile de faire connaître efficacement et en temps opportun bon nombre de ces leçons à l'ensemble de la fonction publique fédérale. Grâce aux Alertes du commissaire à la protection de la vie privée, le Commissariat est en mesure de communiquer ces leçons aux institutions fédérales, tout en respectant ses obligations de confidentialité.

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

Rétrospective de l'exercice



Le Commissariat réalise son mandat en vertu de la LPRPDE par l'entremise de plusieurs activités. Il fait enquête sur les plaintes, surveille la conformité à ses recommandations, collabore avec les autres organisations chargées de l'application de la Loi canadienne anti-pourriel (LCAP), reçoit et examine les déclarations des atteintes à la vie privée, et donne des avis et des conseils aux entreprises, qui continuent de miser sur le potentiel de l'ère numérique pour offrir aux consommateurs de nouveaux produits et services.

Les enquêtes les plus importantes que nous avons menées en 2018-2019 en vertu de la LPRPDE portaient sur le scandale Facebook / Cambridge Analytica et sur l'atteinte à la sécurité des renseignements personnels chez Equifax. Ces dossiers et les autres qui sont résumés dans la présente section illustrent bien les manquements au principe de responsabilité et aux mesures de protection dans les modèles d'affaires émergents. De plus, ils plaident en faveur de la réforme législative que nous réclamons.

Par ailleurs, la déclaration obligatoire des atteintes à la vie privée est entrée en vigueur en 2018-2019. Cette mesure aide le Commissariat à mieux comprendre les types d'atteintes qui se produisent et les risques auxquels sont exposées les entreprises canadiennes.

Mises à jour et tendances en matière de fonctionnement

Au cours de l'exercice, nous avons fermé 282 dossiers de plaintes, dont 178 par règlement rapide.

Le règlement rapide demeure un mécanisme efficace lorsque les problèmes de protection de la vie privée sont simples. Le délai moyen de traitement des dossiers est de moins de trois mois, comparativement à plus d'un an pour un processus d'enquête officielle.

Les plaintes non réglées rapidement mettent de plus en plus en cause des technologies émergentes, des modèles d'affaires novateurs, des répercussions touchant plusieurs territoires de compétence, des enjeux qui recoupent la protection de la vie privée et d'autres domaines comme la protection des consommateurs.

Malgré un effort concerté pour fermer les dossiers de plainte ouverts depuis longtemps, notre arriéré a continué d'augmenter. À la fin de 2018-2019, le nombre de nos enquêtes actives en vertu de la LPRPDE qui remontaient à plus de 12 mois – portant pour la plupart sur des enjeux complexes – est passé de 55 à 64, en hausse de 16 % par rapport à l'exercice précédent.

Le financement temporaire annoncé dans le budget fédéral de 2019 pour remédier à notre arriéré renforcera notre capacité de traiter, au cours des deux prochains exercices, les dossiers de plainte ouverts depuis longtemps.

Les organisations du secteur financier continuent de représenter une part importante (20 %) des plaintes que nous acceptons. Les autres secteurs donnant lieu à une proportion appréciable de plaintes sont ceux des télécommunications (13 %), des services (11 %), d'Internet (10 %) et des transports (10 %). Ces cinq secteurs représentent près des deux tiers des plaintes acceptées.

Comme c'était le cas au cours des années précédentes, les plaintes déposées par les Canadiens portent en grande partie sur l'accès à leurs renseignements personnels (29 %). Viennent ensuite l'utilisation et la communication des renseignements personnels (18 %) et le consentement (17 %).

Facebook refuse de corriger les lacunes constatées en matière de protection de la vie privée

À l'issue d'une enquête du Commissariat sur Facebook en lien avec le scandale de Cambridge Analytica, le géant des médias sociaux a refusé de mettre en œuvre les recommandations visant à corriger de graves lacunes en matière de protection de la vie privée. Cette décision est extrêmement décevante.

Comme nous en avons fait état dans le présent rapport, ce dossier met en évidence l'urgence d'entreprendre une réforme législative.

L'enquête, menée conjointement avec le Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, a révélé que Facebook avait commis des infractions graves aux lois

canadiennes sur la protection des renseignements personnels.

Le commissaire Therrien a souligné une contradiction flagrante entre, d'une part, les promesses publiques faites par Facebook d'améliorer ses pratiques de protection de la vie privée et, d'autre part, son refus de régler les problèmes relevés au cours de l'enquête.

La plainte à l'origine de l'enquête faisait suite à des reportages affirmant que Facebook avait autorisé une organisation à utiliser une application pour avoir accès aux renseignements personnels d'utilisateurs. Par la suite, certains de ces renseignements avaient été communiqués à d'autres organisations, notamment Cambridge Analytica, qui jouait un rôle très actif dans les campagnes électorales aux États-Unis et au Royaume-Uni.

L'application encourageait les internautes à répondre à un test de personnalité. Elle recueillait de l'information sur les utilisateurs qui l'avaient installée ainsi que sur leurs « amis » Facebook. Environ 300 000 utilisateurs de Facebook partout dans le monde avaient téléchargé l'application, ce qui a donné lieu à la communication des renseignements personnels d'environ 87 millions d'utilisateurs, dont plus de 600 000 Canadiens.

L'enquête a donné lieu à plusieurs conclusions importantes, dont les suivantes :

- Les mesures de protection et les mécanismes de consentement superficiels et inefficaces de Facebook ont permis à une application tierce d'avoir accès sans autorisation aux renseignements personnels de millions d'utilisateurs de Facebook. Certains de ces renseignements ont par la suite été utilisés à des fins politiques.
- Facebook a omis d'obtenir un consentement valable des utilisateurs qui installaient l'application et des « amis » de ces utilisateurs, dont les renseignements personnels ont également été communiqués par l'entreprise.
- Facebook n'a pas exercé une bonne surveillance des pratiques de protection de la vie privée des applications sur sa plateforme. Elle s'en est remise aux modalités des ententes conclues avec les responsables des applications pour protéger les utilisateurs contre un accès non autorisé à leurs renseignements. Or, son approche de

surveillance de la conformité à ces modalités était complètement inadéquate.

- Facebook n'a pas été à la hauteur de la responsabilité qui lui incombait en matière de protection des renseignements personnels. Elle a plutôt tenté de transférer cette responsabilité aux applications sur sa plateforme et aux utilisateurs eux-mêmes. Or, selon un des principes de base des lois sur la protection des renseignements personnels, les organisations sont responsables des renseignements personnels qu'elles gèrent.

Facebook a affirmé qu'elle ne donnerait pas suite aux recommandations formulées pour régler ces problèmes. Ce refus entraîne un risque élevé que les renseignements personnels des Canadiens soient utilisés à des fins qu'ils ne connaissent ou ne soupçonnent même pas, ce qui les expose à des préjudices éventuels. Compte tenu de l'énorme quantité de renseignements sensibles confiés à Facebook par les utilisateurs, la situation est extrêmement inquiétante.

Pour ces raisons, le Commissariat a annoncé son intention de demander à la Cour fédérale de rendre une ordonnance contraignante afin d'obliger l'entreprise à corriger ses pratiques de protection de la vie privée.

Ce problème doit absolument être réglé. Il est inadmissible que des organisations puissent faire fi des conclusions de nature juridique formulées par le Commissariat. Il ne devrait pas en revenir à Facebook de décider comment on doit interpréter les lois canadiennes sur la protection des renseignements personnels.

Rapport de conclusions

Enquête portant sur Facebook



Lacunes en matière de sécurité menant à une atteinte massive chez Equifax

Une enquête du Commissariat a révélé que de nombreuses lacunes inacceptables d'Equifax en matière de sécurité avaient ouvert la voie à une atteinte massive à la sécurité des données et en avaient aggravé les répercussions.

Environ 143 millions de personnes partout dans le monde, dont 19 000 Canadiens, ont été touchées par l'atteinte mettant en cause cette agence d'évaluation du crédit.

Les pirates ont eu accès aux systèmes d'Equifax Inc. en mai 2017 en exploitant une vulnérabilité connue de la plateforme du logiciel. Ils ont pu naviguer dans le système d'Equifax sans se faire repérer pendant 77 jours. L'entreprise était au courant de cette vulnérabilité depuis plus de deux mois, mais elle n'y avait pas remédié.

Equifax détient une grande quantité de renseignements personnels très sensibles et joue un rôle clé dans le secteur financier. Des lacunes aussi graves dans les pratiques de protection de la vie privée d'une telle entreprise sont inacceptables.

À la suite de l'atteinte, le Commissariat a reçu 19 plaintes contre Equifax. Il a mené une enquête en deux volets portant à la fois sur Equifax Canada et sa société mère établie aux États-Unis (Equifax Inc.).

L'enquête a révélé diverses lacunes dans le programme de sécurité d'Equifax, dont les suivantes :

- une gestion inadéquate des vulnérabilités pour prévenir les attaques tirant parti de vulnérabilités connues;
- une séparation inadéquate des réseaux pour limiter la portée de l'accès et le préjudice en cas d'incident;
- une mise en œuvre inadéquate des pratiques de base de protection des renseignements pour être en mesure de gérer adéquatement l'utilisation des renseignements personnels et de déceler toute utilisation non autorisée possible.

Fait important, l'enquête a également montré que ni Equifax Canada ni sa société mère n'avaient adopté les mécanismes de surveillance qui auraient dû être en place afin d'évaluer avec précision les risques pour la sécurité et de s'assurer que son programme de sécurité était adéquat pour protéger contre ces risques les renseignements personnels sensibles détenus par Equifax Inc.

Les renseignements personnels des Canadiens détenus par Equifax Inc. aux États-Unis se sont retrouvés en la possession des pirates du fait que ces clients avaient obtenu des services auprès d'Equifax Canada, tels que la surveillance du crédit ou des alertes de fraude. Ces transactions avaient été traitées par la société mère.

Plusieurs plaignants ont déclaré au Commissariat avoir été étonnés d'apprendre que leurs renseignements avaient quitté le Canada et été transférés aux États-Unis.

Le Commissariat a jugé que le transfert de renseignements n'était pas conforme à l'obligation incombant à l'organisation en vertu de la LPRPDE d'obtenir un consentement valable des personnes avant de communiquer leurs renseignements personnels à un tiers. Pour que le consentement soit valable, les personnes doivent obligatoirement recevoir une information claire sur la communication et les risques connexes, y compris lorsque le tiers se trouve dans un autre pays.

Depuis l'incident, Equifax a pris plusieurs mesures pour améliorer ses programmes de sécurité et de responsabilité. L'entreprise a aussi conclu un accord de conformité contraignant en vertu duquel elle s'est engagée à prendre des mesures correctives supplémentaires, et à présenter au Commissariat tous les deux ans, pour une période de six ans, des rapports de vérification, produits par un tiers, portant sur la sécurité d'Equifax Canada et d'Equifax Inc. Ces rapports permettront de surveiller en continu la conformité à la LPRPDE.

Equifax Canada a fini par offrir aux victimes de l'incident une surveillance gratuite de leur crédit pendant une période d'au moins quatre années. Toutefois, elle n'a pas été aussi loin que sa société mère en ce qui concerne les autres protections offertes après l'atteinte à la sécurité des renseignements. En effet, les consommateurs

touchés aux États-Unis ont eu droit à un gel du crédit leur permettant de limiter l'accès à leur dossier de crédit, ce qui réduisait par le fait même le risque de vérification de crédit frauduleuse ou non autorisée.

Rapport de conclusions

Enquête portant sur Equifax

Autres enquêtes majeures

Mise en œuvre par l'Agence mondiale antidopage des recommandations issues de l'enquête

Dans notre rapport annuel 2017-2018, nous analysions les conclusions d'une enquête sur un incident mettant en cause l'Agence mondiale antidopage. Cette organisation établie à Montréal surveille le régime antidopage dans les sports amateurs à l'échelle internationale.

Un groupe de pirates appelé « Fancy Bear » a eu accès à la base de données de l'organisation sur la lutte contre le dopage. Plusieurs gouvernements nationaux, dont celui du Canada, considèrent que ce groupe mène des opérations de cyberespionnage pour le compte de l'État russe par l'intermédiaire de son service de renseignement, soit le GRU.

Le groupe Fancy Bear a communiqué des renseignements sur la santé de plus de 100 athlètes qui avaient participé aux Jeux olympiques de Rio en 2016. Il s'agissait de renseignements sur des problèmes de santé, des médicaments et des analyses d'échantillons de substances corporelles. La base de données de l'Agence renferme d'autres renseignements sensibles, par exemple des renseignements génétiques et des détails sur les allées et venues des athlètes.

L'enquête du Commissariat a révélé que l'organisation n'avait pas mis en place un cadre de sécurité de l'information correspondant à sa situation de cible de grande valeur pour les pirates, dont les groupes commandités par des États. Les mesures de sécurité inadéquates ont rendu l'Agence vulnérable à une

attaque, qui a commencé par une campagne de hameçonnage au cours de laquelle les pirates envoyaient des courriels à ses employés et à d'autres individus ayant accès à la base de données.

Au terme de notre enquête, l'Agence mondiale antidopage a accepté de suivre toutes nos recommandations. Nous avons conclu avec elle un accord de conformité pour surveiller leur mise en œuvre.

Cette année, nous pouvons affirmer que l'organisation a donné suite aux recommandations à notre satisfaction.

Le rapport de conclusions au sujet de l'Agence mondiale antidopage est maintenant accessible au public. L'enquête et le rapport de conclusions comprennent des leçons et de précieux conseils pour d'autres organisations d'envergure, dont les suivants :

- offrir un niveau de protection supérieur aux renseignements très sensibles comme à tout renseignement qui pourrait avoir une grande valeur pour les pirates;
- mettre en place des mesures rigoureuses pour le contrôle de l'accès, par exemple une authentification à deux facteurs, une réinitialisation obligatoire du mot de passe et un système d'alerte pour avertir les utilisateurs lorsque l'on détecte certaines activités inhabituelles dans leur compte;
- chiffrer les renseignements alors qu'ils sont stockés et non seulement au cours de leur transmission;
- s'assurer que le cadre de sécurité de l'information est complet et qu'il comprend une politique écrite, des procédures et une formation;
- communiquer au personnel de l'information sur la sensibilisation à la sécurité dans le cadre de la formation ou par d'autres moyens.

Documents connexes

Rapport de conclusions d'enquête portant sur l'Agence mondiale antidopage

Accord de conformité conclu avec l'Agence mondiale antidopage

Exemple de réussite du règlement rapide

Un individu a déposé contre une banque une plainte portant sur l'inexactitude de renseignements. Il alléguait que la banque avait continué par erreur de transmettre son numéro d'assurance sociale à l'ARC sur les feuillets T5 de sa mère, après qu'il lui eut demandé à plusieurs reprises de corriger l'erreur. Le plaignant avait dû demander une nouvelle cotisation pour un revenu qui n'était pas le sien. Notre enquêteur a contacté la banque, ce qui a permis de trouver la cause du problème et d'apporter les correctifs voulus. Le Commissariat a chapeauté une rencontre entre le plaignant et la banque, ce qui a permis de clore le dossier.

Imposition de frais pour supprimer des numéros d'un annuaire téléphonique en ligne

L'entreprise 411Numbers HK Ltd. (411Numbers), constituée en personne morale à Hong Kong mais gérée à partir du Québec, exploitait plus d'une dizaine de sites Web donnant accès gratuitement au numéro de téléphone et à d'autres renseignements d'individus au Canada et dans d'autres pays. Elle génère des revenus grâce à la publicité. Auparavant, elle en tirait en imposant des frais pour supprimer les renseignements des individus.

Le plaignant alléguait que 411Numbers avait recueilli, utilisé et communiqué son nom, son adresse et son

numéro de téléphone confidentiel à son insu et sans son consentement pour afficher ces renseignements sur le site Web de l'entreprise.

Il s'opposait également à ce que 411Numbers utilise ses renseignements pour générer des revenus en offrant un service de suppression moyennant des frais et en exigeant que les individus fournissent davantage de renseignements que nécessaire afin d'avoir recours à ce service. Pour faire retirer des renseignements personnels du site Web, 411Numbers exigeait une photocopie du passeport, du permis de conduire et d'une facture d'une entreprise de services publics. De plus, le plaignant accusait l'entreprise de ne pas répondre à ses questions concernant la protection de la vie privée. D'ailleurs, le Commissariat a corroboré cette allégation, car nous avons nous-mêmes eu, au début, beaucoup de difficulté à contacter l'entreprise.

411Numbers affirmait que le Commissariat n'avait pas compétence pour faire enquête dans ce dossier sous prétexte qu'elle avait été constituée en personne morale en vertu des lois de Hong Kong et que ses serveurs se trouvaient à l'extérieur du Canada. Toutefois, l'enquête a révélé un lien réel et important entre les activités de 411Numbers et le Canada, d'après les éléments découverts montrant qu'elle exerçait en réalité ses activités à partir d'ici.

L'entreprise a aussi fait valoir que le public avait accès aux renseignements en question, si bien qu'aucun consentement n'était requis pour les afficher sur ses sites Web. Le Commissariat a rejeté cet argument. En effet, le public a accès aux noms, adresses et numéros de téléphone publiés dans l'annuaire pages blanches d'une société de télécommunications, mais non aux numéros de téléphone confidentiels. Le consentement des individus à la collecte, à l'utilisation et à la communication de ces renseignements est donc nécessaire.

Par suite de cette enquête, les renseignements personnels du plaignant ont été supprimés du site Web et 411Numbers a mis fin à sa pratique consistant à imposer des frais à cette fin. Les individus qui demandent la suppression de leurs renseignements du service d'annuaire peuvent maintenant le faire en remplissant simplement un formulaire en ligne. Comme l'entreprise a cessé d'imposer des frais pour supprimer les renseignements, nous avons estimé que cet aspect du dossier était résolu. Nous avons toutefois remarqué

que la publication de renseignements personnels, sans consentement, dans le but d'inciter les intéressés à acquitter des frais pour faire supprimer cette information, serait probablement considérée comme non appropriée en vertu de la LPRPDE.

Enfin, nous avons constaté que les gens avaient beaucoup de difficulté à contacter 411Numbers, que l'entreprise n'était pas suffisamment au courant des obligations lui incombant en vertu de la LPRPDE et que sa politique de confidentialité renfermait plusieurs erreurs.

Le Commissariat a formulé plusieurs recommandations, que 411Numbers a accepté de mettre en œuvre. L'entreprise s'est engagée :

- à supprimer les renseignements associés aux numéros de téléphone confidentiels sur tous ses sites Web;
- à mettre en œuvre des mesures de diligence raisonnable pour s'assurer que les listes obtenues à l'avenir ne renferment aucun numéro de téléphone confidentiel;
- à mettre en œuvre des mesures pour améliorer sa responsabilité, sa transparence et sa capacité de répondre au souhait des individus qui veulent contester sa conformité à la Loi.

Au cours de notre enquête, une autorité européenne de protection des données ayant reçu des plaintes similaires contre 411Numbers déposées par plusieurs individus a sollicité notre assistance. L'entreprise a également accepté à l'issue de notre enquête de supprimer du site les renseignements personnels de ces plaignants.

Au moment de la rédaction du présent rapport, aucun des sites Web non canadiens de l'entreprise n'est en service, les renseignements concernant plus d'un million de Canadiens ont été retirés du site Web canadien, et nous sommes toujours en communication avec l'entreprise pour nous assurer que l'ensemble de nos recommandations seront pleinement adoptées.

Loi canadienne anti-pourriel (LCAP)

Le Commissariat à la protection de la vie privée partage avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence la responsabilité de mettre en application la LCAP. Les trois organismes ont travaillé en collaboration et se sont réunis régulièrement avec des partenaires nationaux et internationaux pour promouvoir la conformité à la loi au cours de l'exercice écoulé.

En 2018-2019, le Commissariat a travaillé en collaboration avec les autres organismes chargés de l'application de la LCAP afin d'appuyer le lancement et la publication d'un nouveau rapport de mesure du rendement qui donne des renseignements plus utiles aux entreprises, et de moderniser le site Web combattrelepourriel.gc.ca d'ISDE destiné au grand public.

Le Commissariat est membre du Unsolicited Communications Enforcement Network (UCENet), réseau regroupant des autorités chargées de la lutte contre les pourriels, de la protection des consommateurs et de la réglementation des télécommunications. Le Commissariat a contribué aux discussions qui ont mené à l'élaboration du plan opérationnel du réseau pour la période allant de 2019 à 2021. Le Commissariat a également pris part aux réunions annuelles conjointes 2018 d'UCENet et du Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), auxquelles prennent part les spécialistes de la sécurité des TI du secteur privé. À ces rencontres conjointes, le Commissariat a présenté une étude technologique réalisée dans le cadre d'une enquête sur les publiciels, ainsi qu'un survol de ses activités et de son mandat en lien avec la LCAP.

Le Commissariat a poursuivi son offre de conseils concernant la conformité à la LCAP à l'intention des entreprises et des particuliers par l'entremise de différents canaux. En 2018-2019, le Commissariat a mis à jour ses ressources en ligne se rapportant à la LCAP, notamment les outils qui aident les entreprises à se conformer à cette loi ainsi qu'une page Web générale consacrée à la LCAP. Le Commissariat a aussi lancé et fait connaître une nouvelle trousse de présentation sur la LPRPDE pour les entreprises. On y trouve de l'information sur la LCAP et la manière

Rapport de conclusions

Enquête portant sur 411Numbers

dont elle s'applique au cybermarketing. En outre, des représentants du Commissariat ont tenu des stands ou pris la parole à l'occasion de plusieurs activités portant sur la LCAP et distribué de la documentation sur le sujet aux entreprises.

Le Centre d'information du Commissariat a reçu 78 demandes d'information, présentées par des individus et des entreprises, concernant la LCAP. Les trois types de demandes les plus courantes portaient sur la façon de signaler des messages non sollicités, la façon de se désabonner de listes de diffusion par courriel, ainsi que l'applicabilité de la LCAP et les mesures à prendre pour s'y conformer.

Mise à jour sur les déclarations d'atteintes

La déclaration obligatoire des atteintes à la vie privée sous le régime de la LPRPDE est entrée en vigueur le 1^{er} novembre 2018. Depuis cette date, le nombre de déclarations a augmenté de près de 500 %.

Au chapitre des tendances, nous constatons une hausse du nombre de déclarations d'atteintes à la vie privée ne touchant que quelques personnes. Les organisations doivent maintenant signaler toute atteinte à la vie privée qui atteint le seuil de déclaration sous le régime en vigueur, peu importe le nombre d'individus touchés. En vertu du régime antérieur de déclaration volontaire, nous recevions relativement peu de déclarations d'atteintes à la vie privée ne touchant qu'un petit nombre de personnes.

La majorité des atteintes signalées résultaient d'un accès non autorisé (62 %), c'est-à-dire qu'elles avaient été commises par des malfaiteurs ou par des employés indiscrets. D'après une première analyse des déclarations d'atteintes à la vie privée en vertu de la LPRPDE, les indiscretions d'employés et le piratage psychologique sont souvent à l'origine des incidents découlant d'un accès non autorisé. Le piratage psychologique repose sur le hameçonnage ciblé ou l'usurpation d'identité, parfois en utilisant des données personnelles ou des données de connexion ayant fait l'objet d'une fuite au cours d'un incident antérieur, dans le but de s'emparer des comptes d'un autre individu pour en tirer un gain financier.

Nous constatons encore des atteintes mettant en cause, entre autres, des communications à des membres de la famille, la perte ou le vol d'appareils, l'installation de logiciels malicieux, des attaques visant la vulnérabilité des réseaux, les demandes de connexion automatisée à grande échelle, les attaques par force brute, et les communications accidentelles (telles l'insertion de listes d'adresses de courriel dans le champ « copie conforme » plutôt que dans le champ « copie conforme invisible »).

Toutefois, dans de nombreux cas, il est possible que les entreprises pêchent par excès de prudence en signalant des atteintes qui ne semblent pas poser « un risque réel de préjudice grave », ce qui constitue le seuil de déclaration. De fait, 33 % des atteintes déclarées entre novembre 2018 et la fin de mars 2019 semblent se situer en deçà de ce seuil. Bien que le Commissariat évalue les signalements au cas par cas, dans certains dossiers, les entreprises ont signalé des atteintes où aucun renseignement personnel n'avait été compromis, ou d'autres encore où des malfaiteurs avaient tenté sans succès de contourner les mesures de sécurité.

Le Commissariat a élaboré un document d'orientation pour aider les organisations à se conformer aux nouvelles exigences. Ce document aborde des questions d'ordre général, soit les étapes à entreprendre en cas d'atteinte, la création d'un registre et le signalement aux personnes touchées.

Au moment de la rédaction du présent rapport, nous avons entrepris un examen des registres d'atteintes comme première évaluation sur le terrain de la conformité aux exigences obligatoires en matière d'atteintes. En plus d'imposer le respect des règles, cet exercice nous aidera à déterminer les enjeux qui pourraient faire l'objet de lignes directrices, par exemple l'interprétation du risque réel de préjudice grave, les omissions de signalement et la conservation déficiente de registres.

Conseils aux entreprises

La Direction des services-conseils à l'entreprise a été créée en 2018 afin d'aider les entreprises à mieux comprendre les répercussions des nouvelles technologies et des nouveaux modèles d'affaires sur la vie privée ou à évaluer les répercussions de leurs pratiques actuelles sur la vie privée.

Nous estimons que des pouvoirs d'application de la loi renforcés devraient faire partie d'un cadre législatif moderne, mais que l'application de la loi ne devrait pas être la principale stratégie utilisée pour favoriser la conformité. La création de la Direction des services-conseils à l'entreprise s'inscrit dans un virage global visant à centrer nos activités sur des efforts proactifs accrus.

Le Commissariat privilégie le règlement des questions de protection de la vie privée dès le début et la résolution des problèmes en collaboration, en dehors du processus officiel d'application de la Loi. Cette approche évite des enquêtes longues et coûteuses et aide à réduire, par la suite, les risques d'atteinte à la vie privée. De plus, elle offre aux institutions une certaine uniformité et une certaine prévisibilité dans leurs rapports avec le Commissariat et permet à tous de tirer parti de l'innovation.

La Direction peut offrir ses services-conseils de façon proactive, mais toutes les entreprises assujetties à la LPRPDE ont la possibilité de consulter ses spécialistes. Jusqu'à présent, la réaction du secteur privé est très positive.

Au cours de l'exercice écoulé, le Commissariat a donné des conseils et rencontré des responsables de la protection de la vie privée de diverses entreprises commerciales. Lors de ces rencontres, il leur a fait part de pratiques exemplaires qu'elles peuvent adopter pour obtenir le consentement valable requis afin d'utiliser les renseignements des clients et pour limiter la collecte inappropriée de renseignements.

De façon générale, les services-conseils offerts par le Commissariat sont visés par les dispositions de la LPRPDE concernant la confidentialité. Dans des cas particuliers, certains renseignements pourront être communiqués si c'est dans l'intérêt public. Les exemples présentés ci-après illustrent le travail effectué en 2018-2019 par la Direction des services-conseils à l'entreprise.

Projet Apple Maps

Le projet de récupération des images pour Apple Maps vise à cartographier des rues et à effectuer des études de terrain. Il est mené dans divers pays, dont le Canada, afin de recueillir de nouvelles données pour améliorer Apple Maps. De son propre chef, Apple a eu recours aux services-conseils du Commissariat concernant ce projet. Les dispositions de la LPRPDE régissant la confidentialité nous interdisent de communiquer le détail des discussions, mais nous pouvons affirmer qu'Apple a été très réceptive à nos recommandations initiales et qu'elle poursuit son dialogue avec le Commissariat.

Projet du Quayside de Sidewalk Labs à Toronto

Sidewalk Labs a l'intention d'aménager un quartier de 12 acres sur la rive du lac Ontario, à Toronto, dans le secteur Quayside. Waterfront Toronto, organisme fondé et financé par trois ordres de gouvernement, est son partenaire dans ce projet. Sidewalk Labs est une filiale d'Alphabet Inc., société mère de Google.

Les médias nationaux ont largement fait état des répercussions que pourrait avoir sur la vie privée ce projet de haute technologie. Les critiques étaient partagées sur la question de savoir si les avantages escomptés de l'initiative, soit le développement durable et la qualité de vie, l'emporteraient sur le risque de surveillance de masse de citoyens canadiens par un géant de la technologie américain.

Le Commissariat examine actuellement le plan directeur d'innovation et de développement du projet publié en juin 2019 par Waterfront Toronto. S'il y a lieu, nous formulerons nos commentaires et recommandations sur les aspects de ce plan qui relèveraient de la LPRPDE. Compte tenu de la nature révolutionnaire du projet et de son importance pour l'avenir de l'aménagement urbain au Canada et ailleurs, le Commissariat continue de suivre l'évolution du dossier et de dialoguer de façon proactive avec les parties intéressées pour formuler les commentaires et les avis que nous jugerons pertinents.

Programme des contributions

Au moyen de son Programme des contributions, le Commissariat finance la recherche indépendante et les initiatives connexes d'application des connaissances sur la protection de la vie privée. Ce programme vise à générer des idées, approches et connaissances nouvelles dans le domaine qui pourraient aider, d'une part, les organisations à mieux protéger les renseignements personnels et, d'autre part, les Canadiens à prendre des décisions plus éclairées concernant la protection de leur vie privée.

Nous lançons chaque automne un appel de propositions. Les établissements universitaires et les organismes à but non lucratif, notamment les associations industrielles, les organismes de protection des consommateurs, les organismes bénévoles, les associations professionnelles et les organismes de défense des intérêts, sont admissibles au financement. Le budget du Programme des contributions s'élève à 500 000 \$ par an.

Le Commissariat a reçu 29 propositions pour le cycle de financement 2018-2019. Ces propositions ont été évaluées par le Commissariat lui-même ainsi que par un comité externe d'évaluation par les pairs. À l'issue de l'évaluation, neuf projets ont été retenus.

Les projets financés en 2018-2019 portent sur un large éventail d'enjeux, dont les suivants :

- une étude de l'Université de Toronto sur les logiciels traqueurs, type de logiciels de surveillance portant atteinte à la vie privée qu'une personne installe sur un appareil d'un proche dans le but de le harceler ou de lui faire subir de la violence dans le cadre d'une relation intime;
- une étude de l'Université McMaster aidant à mieux comprendre les répercussions sur la vie privée des villes intelligentes au Canada;
- une étude d'Option consommateurs explorant les répercussions, sur la vie privée, du partage d'images et de renseignements personnels d'enfants par leurs parents dans les médias sociaux;

- un projet de la BC Society of Transition Houses visant à donner aux organismes canadiens de lutte contre la violence faite aux femmes et aux enfants des conseils en matière de vie privée et de sécurité liés à l'utilisation de bases de données électroniques;
- une étude de l'Université Concordia sur les fuites de renseignements personnels dans les réseaux Wi-Fi publics.

La recherche indépendante que nous finançons sous l'égide du Programme des contributions est utile pour le travail que nous réalisons au Commissariat. Par exemple, la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC) a étudié en 2018 les répercussions, sur la vie privée, de l'industrie canadienne des courtiers en données. Dans le cadre de son enquête en cours sur cette industrie, le Commissariat utilise de l'information issue du projet de recherche de la CIPPIC.

Devant les tribunaux

Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN) c. Procureur général du Canada, décision n° A-463-16 (Cour d'appel fédérale)

Le Syndicat des agents correctionnels du Canada a porté en appel la décision rendue par la Cour fédérale (2016 CF 1289), selon laquelle les vérifications de crédit obligatoires pour les agents correctionnels, comme l'exige la nouvelle Norme sur le filtrage de sécurité du Secrétariat du Conseil du Trésor (la Norme), ne contreviennent pas à la LPRP ni à la *Charte canadienne des droits et libertés*. La Cour fédérale a également conclu que l'article 4 de la LPRP n'exige pas que la collecte des renseignements personnels soit **nécessaire** aux programmes ou aux activités d'une institution fédérale.

Le Commissariat a obtenu le statut d'intervenant dans l'appel. Il a présenté des observations concernant l'interprétation de l'article 4 de la LPRP, notamment le fait que cet article impose bel et bien un critère de nécessité aux institutions fédérales pour la collecte des renseignements personnels et la question de savoir si le Syndicat était autorisé à invoquer une infraction à l'article 4 en demandant un contrôle judiciaire.

R. c. Jarvis, 2019 CSC 10

Cette affaire met en cause un enseignant d'une école secondaire qui a utilisé un stylo-caméra pour produire subrepticement des enregistrements vidéo de plusieurs élèves de sexe féminin à l'école où il enseignait. Nombre des vidéos visaient la poitrine et le décolleté de ces élèves. L'enseignant a été accusé de voyeurisme en

application du paragraphe 162(1) du *Code criminel*. Il a cependant été acquitté à son procès parce que la Couronne n'avait pas réussi à prouver hors de tout doute raisonnable que les enregistrements avaient été produits dans un « but sexuel ».

En deuxième instance, la Cour d'appel de l'Ontario a conclu à l'unanimité que les enregistrements avaient été produits dans un « but sexuel ». Toutefois, dans une décision majoritaire, les juges ont conclu que les élèves filmées par l'intimé ne se trouvaient pas « dans des circonstances pour lesquelles il existe une attente raisonnable de protection en matière de vie privée ». Par conséquent, cet élément constitutif de l'infraction de voyeurisme n'avait pas été prouvé. Le raisonnement des juges majoritaires repose sur le fait que les élèves se trouvaient dans un lieu public (c'est-à-dire à l'intérieur et autour de l'école) lorsque les enregistrements ont été produits. Ainsi, elles devaient s'attendre à être observées et filmées. Le juge Huscroft, dissident dans la cause, a conclu que les élèves avaient une attente raisonnable de protection en matière de vie privée par rapport à quiconque cherchant à compromettre leur intégrité personnelle et sexuelle pendant qu'elles étaient à l'école. Il aurait donc accueilli l'appel.

En s'appuyant sur la dissidence du juge Huscroft, la Couronne a porté en appel de plein droit devant la Cour suprême du Canada la décision de la Cour d'appel de l'Ontario.

Le Commissariat et plusieurs autres organismes ont obtenu le statut d'intervenant. Le Commissariat a soutenu que le concept d'attente raisonnable de protection en matière de vie privée dans le contexte de l'infraction de voyeurisme devait être évalué en

fonction de l'ensemble des circonstances. Il a fait valoir que l'interprétation étroite et tribulaire d'un lieu adoptée par les juges majoritaires de la Cour d'appel de l'Ontario était erronée et qu'elle porterait atteinte au droit à la vie privée des Canadiens dans nombre de contextes.

Dans sa décision, la Cour suprême du Canada a confirmé une interprétation contextuelle de la protection en matière de vie privée dans des lieux publics dans le contexte de l'infraction de voyeurisme. Elle a reconnu que le concept de vie privée n'est pas absolu et qu'une personne ne renonce pas à son droit à la vie privée simplement parce qu'elle se trouve dans un lieu public ou semi-public.

La Cour a également souligné dans son arrêt que, pour déterminer s'il y a eu atteinte au droit à la vie privée d'une personne, il faut examiner ces affaires au cas par cas, en tenant compte de toutes les circonstances particulières. À cet égard, elle a réaffirmé que la vie privée doit être évaluée en fonction des technologies en évolution, lesquelles peuvent faciliter la tâche des agents de l'État ou des particuliers qui veulent « recueillir, conserver et diffuser des renseignements » sur des personnes. La Cour a aussi indiqué que nos attentes raisonnables de protection en matière de vie privée ne devraient pas diminuer au même rythme que cette évolution.

De façon plus générale, la Cour s'est montrée sensible à l'importance du droit à la vie privée en jeu, soit la protection du corps de jeunes personnes et leur attente raisonnable de ne pas être filmées dans un but sexuel par une personne en situation de confiance.

Renvoi visant Google (T-1779-18)

Le commissaire à la protection de la vie privée du Canada a présenté, en vertu de l'article 18.3 de la *Loi sur les Cours fédérales*, une demande de renvoi de deux questions pour audition et jugement :

Dans l'exploitation de son service de moteur de recherche, est-ce que Google LLC (Google) recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales, au sens de l'alinéa 4(1)a) de la *Loi sur la protection des renseignements personnels et les documents électroniques* L.C. 2000, ch. 5 (« LPRPDE » ou

la « Loi »), lors de l'indexation de pages Web et de la présentation des résultats de recherches concernant le nom d'un individu?

L'exploitation du service de moteur de recherche de Google est-elle exclue du champ d'application de la partie 1 de la LPRPDE, selon les termes de l'alinéa 4(2)c) de la LPRPDE, parce que par une telle exploitation Google recueille, utilise et communique des renseignements personnels à des fins journalistiques, artistiques ou littéraires et à aucune autre fin?

Ces questions ont été soulevées dans le contexte d'une plainte déposée par un individu alléguant que Google contrevient à la LPRPDE en continuant d'afficher de manière visible des liens menant à des articles de presse en ligne le concernant dans les résultats de recherches lorsque l'on fait une recherche concernant son nom au moyen du service de moteur de recherche de l'entreprise. Le plaignant a demandé à Google de retirer les articles en question des résultats de recherches concernant son nom.

Dans sa réponse initiale à la plainte, Google a soutenu ne pas être assujettie à la LPRPDE dans les circonstances. Avant de poursuivre l'enquête, le commissaire a voulu déterminer si la LPRPDE s'applique à l'exploitation par Google de son moteur de recherche. C'est pourquoi il a d'abord renvoyé à la Cour pour jugement les deux questions susmentionnées afin de trancher le conflit de compétence.

Peu après le dépôt du renvoi, Google a demandé au tribunal d'en élargir la portée pour statuer également sur la question de savoir si une éventuelle exigence imposant la suppression des liens de ses résultats de recherches contreviendrait à l'alinéa 2b) de la *Charte canadienne des droits et libertés* ou, autrement, de faire annuler le renvoi. Le 16 avril 2019, la Cour a rejeté la requête de Google, qui a interjeté appel de la décision. Elle a rejeté cet appel le 22 juillet 2019. La décision sur le fond n'avait pas encore été rendue au moment de la rédaction du présent rapport.

Le Commissariat a indiqué qu'il ne finaliserait pas son Projet de position sur la réputation en ligne avant la conclusion de la procédure de renvoi.

Coalition canadienne pour l'équité génétique c. Procureure générale du Québec, et al. (CSC 38478)

Cette affaire porte sur une procédure de renvoi instituée par le gouvernement du Québec concernant la validité constitutionnelle de la *Loi sur la non-discrimination génétique*, L.C. 2017, ch. 3, (LNDG), qui interdit certaines pratiques dangereuses liées à la collecte, à l'utilisation ou à la communication des résultats de tests génétiques.

Plus particulièrement, la LNDG crée des interdictions distinctes concernant les tests génétiques obligatoires ainsi que la collecte, l'utilisation et la communication des résultats de tests génétiques sans consentement (articles 1 à 7). Cette loi a également modifié le *Code canadien du travail* (article 8) et la *Loi canadienne sur les droits de la personne* (articles 9 et 10) pour protéger les employés sous réglementation fédérale à l'égard des tests génétiques et les protéger contre la discrimination fondée sur des caractéristiques génétiques.

Peu après l'adoption de cette loi, le gouvernement du Québec a renvoyé à la Cour d'appel du Québec la question de la validité constitutionnelle des articles 1 à 7 de la LNDG (mais non les modifications apportées au *Code canadien du travail* ou à la *Loi canadienne sur les droits de la personne*). Le renvoi porte sur la question de savoir si les articles 1 à 7 de la LNDG dépassent le pouvoir du législateur de légiférer en matière criminelle en vertu de la *Loi constitutionnelle de 1867*.

Les dispositions de la LNDG en cause interdisent :

- d'obliger une personne à subir un test génétique comme condition préalable à la fourniture de biens ou de services ou à la conclusion ou au maintien d'un contrat ou de ses modalités ou encore de lui refuser d'exercer l'une de ces activités au motif qu'elle a refusé de subir un test génétique (article 3);
- d'obliger une personne à communiquer les résultats d'un test génétique comme condition préalable à l'exercice de l'une de ces activités ou de lui refuser d'exercer l'une de ces activités au motif qu'elle a refusé de les communiquer (article 4);

- de recueillir, d'utiliser ou de communiquer à quiconque fournit des biens ou des services à une personne ou conclut ou maintient un contrat avec elle les résultats d'un test génétique sans le consentement écrit de la personne visée (article 5).

L'article 6 exempte les professionnels de la santé et les chercheurs de l'application des articles 3 à 5. En vertu de l'article 7, quiconque contrevient à l'un des articles 3 à 5 commet une infraction pouvant entraîner une amende et un emprisonnement.

Dans sa décision, la Cour d'appel du Québec a conclu à l'unanimité que les dispositions en cause dépassaient le pouvoir du législateur de légiférer en matière criminelle.

La Coalition canadienne pour l'équité génétique, qui a le statut d'intervenant devant la Cour d'appel du Québec, a porté en appel de plein droit devant la Cour suprême du Canada les décisions de la Cour.

La procureure générale du Québec et la procureure générale du Canada, qui ne défendaient pas non plus la validité constitutionnelle de la LNDG devant la Cour d'appel du Québec, sont intimées dans l'appel. Le Commissariat, les procureurs généraux de la Colombie-Britannique et de la Saskatchewan, l'Association canadienne des compagnies d'assurances de personnes, la Commission canadienne des droits de la personne et le Collège canadien de généticiens médicaux ont le statut d'intervenant dans l'appel.

Au moment de la rédaction de ce rapport, la date de l'audition de l'appel était provisoirement fixée au 10 octobre 2019.

Certains documents d'orientation publiés par le Commissariat concernant la collecte, l'utilisation et la communication des résultats de tests génétiques font référence à la LNDG. Ils seront mis à jour lorsque la Cour suprême du Canada aura rendu sa décision dans cette affaire.

Coopération avec des autorités canadiennes et étrangères

La protection de la vie privée constitue de plus en plus un défi d'envergure mondiale dans notre monde numérisé, alors que les effets bénéfiques – et néfastes – de la technologie transcendent désormais les frontières. D'énormes quantités de renseignements personnels peuvent maintenant transiter à tout instant entre les pays du monde entier.

En cette ère d'innovation continue et de complexité technologique croissante, une coopération internationale axée sur le déploiement d'efforts concertés pour résoudre les questions communes de protection de la vie privée est essentielle pour protéger le droit à la vie privée des citoyens. Le partage des responsabilités et de la charge de travail entre les autorités de protection de la vie privée élargit le rayon d'action de chacune d'entre elles. En collaborant, les partenaires peuvent tirer parti des points forts de la législation des différents pays, y compris leurs pouvoirs d'application de la réglementation, pour assurer des pratiques de conformité plus efficaces et globales.

Les autorités de protection des données ne peuvent faire progresser leurs objectifs de protection de la vie privée en faisant cavalier seul. Nombre de pays et de régions en développement qui adoptent maintenant de nouvelles lois sur la protection de la vie privée ou sont en voie de créer un régime de réglementation dans le domaine se tournent vers les pays bien établis, comme le Canada, pour obtenir de l'aide et de l'information concernant les pratiques exemplaires.

Au bout du compte, la participation du Commissariat à ce type d'initiatives internationales aide à mieux protéger les Canadiens. Des droits à la vie privée mieux garantis dans d'autres régions du monde aident à faire en sorte que les Canadiens soient mieux protégés lorsque leurs

renseignements personnels sont transférés à l'étranger aux fins de traitement.

En décembre 2018, le commissaire Therrien a participé à une réunion du Comité contre le terrorisme du Conseil de sécurité des Nations Unies, à New York. Les participants y ont discuté des défis à relever pour protéger la vie privée et les renseignements personnels, tout en luttant efficacement contre le terrorisme.

Dans son allocution, le commissaire a souligné que la protection de la vie privée constitue un droit de la personne reconnu à l'échelle internationale et que les mesures de lutte contre le terrorisme faisant appel à la collecte, à la communication et à l'analyse des renseignements personnels doivent respecter ce droit. Il a également fait valoir l'importance de la nécessité, de la proportionnalité et d'une surveillance indépendante – trois principes au cœur de la plupart des lois sur la protection de la vie privée et des données, qui sont particulièrement pertinents dans le contexte de la sécurité nationale.

Le Commissariat collabore régulièrement avec les organismes de réglementation de la protection de la vie privée d'autres pays. Dans certains cas, il leur vient en aide en communiquant des données probantes à l'appui de mesures d'application de la loi unilatérales; dans d'autres, il fait équipe avec des autorités dans le cadre d'enquêtes conjointes. Par exemple, en 2018-2019, l'enquête du Commissariat sur 411Numbers a permis de répondre aux préoccupations d'individus qui avaient déposé une plainte auprès de l'autorité de protection des données de l'Allemagne.

Dans le dossier Equifax, le Commissariat a bénéficié de la collaboration de la Federal Trade Commission des États-Unis et du Information Commissioner's Office du

Royaume-Uni. Il ne s'agissait pas à proprement parler d'enquêtes conjointes, mais nous avons échangé de l'information avec ces deux organismes dans le cadre de notre analyse. De même, notre enquête sur Facebook a tiré parti de l'échange d'information avec l'Information Commissioner's Office du Royaume-Uni.

Des relations solides font également partie intégrante de notre travail sur la scène nationale. Nous avons conclu des [protocoles d'entente avec plusieurs provinces](#) pour consulter leur commissaire à la protection de la vie privée et échanger avec lui de l'information pertinente. Ces protocoles, qui aident à offrir aux Canadiens un système de contrôle et de protection des renseignements personnels aussi homogène que possible, ont été conclus avec le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, ainsi qu'avec le Commissaire à l'information et à la protection de la vie privée de l'Ontario. Par exemple, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique nous a permis d'adapter pour notre propre site Web son [document d'orientation sur la protection de la vie privée dans le contexte de l'achat et de la vente de cannabis](#) à la suite de la légalisation de la marijuana au Canada.

Au cours de l'exercice écoulé, le Commissariat a participé à un plus grand nombre d'enquêtes menées en collaboration avec des partenaires canadiens. Ainsi, l'enquête du Commissariat sur Facebook, Inc. a été menée conjointement avec le commissariat de la Colombie-Britannique. En outre, nous faisons actuellement enquête sur le recours à la technologie de reconnaissance faciale dans les centres commerciaux conjointement avec les commissariats de l'Alberta et de la Colombie-Britannique et la Commission d'accès à l'information du Québec.

Le Commissariat s'efforce aussi de travailler en collaboration avec les organismes provinciaux et territoriaux analogues sur les enjeux communs touchant l'éducation du public et la politique dans les secteurs public et privé. Dans le cadre des efforts concertés que nous déployons tous pour protéger et promouvoir le droit à la vie privée, nous déposons à l'occasion des

résolutions conjointes pour souligner notre consensus sur des questions de politique publique et exprimer nos préoccupations ou notre soutien communs sur certains enjeux qui préoccupent les Canadiens. Cette concertation des commissaires à l'information et à la protection de la vie privée est avantageuse pour les Canadiens, car elle lance un appel à l'action qui favorisera des mesures de protection de la vie privée uniformes pour les individus dans l'ensemble du pays.

Au cours de leur réunion annuelle tenue en septembre 2018 à Regina, en Saskatchewan, les commissaires à l'information et à la protection de la vie privée fédéraux, provinciaux et territoriaux ont adopté une [résolution conjointe invitant les gouvernements à adopter une loi obligeant les partis politiques à respecter les principes de protection de la vie privée reconnus mondialement](#). Le but est d'assurer l'accès des Canadiens aux renseignements personnels que détiennent leurs organismes respectifs au sujet des intéressés, d'autoriser un organisme de surveillance indépendant à vérifier la conformité aux règles en matière de protection de la vie privée et de veiller à leur application.

Cette résolution souligne le manque d'uniformité des dispositions s'appliquant aux partis politiques au Canada. Elle invite les gouvernements à adopter des lois sur les pratiques de surveillance susceptibles d'avoir d'importantes répercussions sur la vie privée des citoyens et de miner leur confiance à l'égard du système démocratique. La résolution s'ajoute à la déclaration du Commissariat portant sur cet enjeu et sur la nécessité d'une réforme législative, prononcée devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, pour l'étude de l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et à Facebook. Tout cela renseigne les parlementaires et les aide à mieux protéger le droit à la vie privée des Canadiens.

Annexe 1 : Définitions

Types de plainte

Accès

À la suite d'une demande officielle d'accès à l'information, l'institution ou l'organisation aurait refusé à une ou à plusieurs personnes l'accès aux renseignements personnels qu'elle détient à leur sujet.

Avis de prorogation

En vertu de la LPRP, l'institution n'aurait pas donné une justification appropriée pour la prorogation, aurait fait la demande de prorogation après le délai initial de 30 jours ou aurait fixé l'échéance à plus de 60 jours après la date de réception de la demande.

Collecte

L'institution ou l'organisation aurait recueilli des renseignements personnels non nécessaires ou les aurait recueillis par des moyens inéquitables ou illicites.

Consentement

En vertu de la LPRPDE, une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement valable de la personne en cause ou, pour le motif qu'elle fournit un bien ou un service, a exigé que la personne consente à une collecte, à une utilisation ou à une communication déraisonnable de renseignements personnels.

Conservation et retrait

L'institution ou l'organisation n'aurait pas conservé des renseignements personnels selon le calendrier de conservation pertinent – les renseignements auraient été détruits trop rapidement ou conservés trop longtemps.

Correction ou annotation (accès)

L'institution ou l'organisation n'aurait pas corrigé des renseignements personnels ou, en cas de désaccord avec les corrections demandées, n'aurait pas annoté le dossier pour en faire état.

Correction ou annotation (délais)

En vertu de la LPRP, l'institution n'aurait pas corrigé les renseignements personnels ou n'aurait pas annoté le dossier en conséquence dans les 30 jours suivant la réception de la demande de correction.

Délais

L'institution n'aurait pas répondu à une demande dans les délais prescrits par la LPRP.

Détermination des fins de la collecte des renseignements

En vertu de la LPRPDE, une organisation n'a pas déterminé les fins de la collecte de renseignements personnels avant la collecte ou au moment de celle-ci.

Exactitude

L'institution ou l'organisation n'aurait pas pris toutes les mesures raisonnables pour s'assurer que les renseignements personnels utilisés sont exacts, à jour et complets.

Frais

L'institution ou l'organisation aurait exigé indûment des frais pour répondre à une demande d'accès à des renseignements personnels.

Langue

En réponse à une demande présentée en vertu de la LPRP, l'institution ou l'organisation n'aurait pas fourni les renseignements personnels dans la langue officielle choisie par le demandeur.

Mesures de protection

En vertu de la LPRPDE, une organisation n'a pas protégé par des mesures de protection appropriées les renseignements personnels qu'elle détient.

Possibilité de porter plainte

En vertu de la LPRPDE, une organisation n'a pas mis en place des procédures ou des politiques permettant à une personne de porter plainte à l'égard du non-respect de la Loi ou elle a enfreint ses propres procédures et politiques.

Répertoire

InfoSource (un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données – groupes de fichiers sur le même sujet – qu'elle possède) ne décrirait pas de façon adéquate le fonds de renseignements personnels d'une institution.

Responsabilité

En vertu de la LPRPDE, une organisation ne s'est pas acquittée de ses responsabilités à l'égard des renseignements personnels en sa possession ou sous sa garde ou elle n'a pas désigné une personne responsable de s'assurer qu'elle se conforme à la Loi.

Transparence

En vertu de la LPRPDE, une organisation n'a pas rendu facilement accessibles aux demandeurs des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Utilisation et communication

L'institution ou l'organisation aurait utilisé ou communiqué des renseignements personnels sans le consentement de la personne en cause ou les aurait utilisés ou communiqués de façon non conforme aux usages et aux communications prévus par la loi.

Décisions

Fondée

L'institution ou l'organisation a enfreint une disposition de la LPRP ou de la LPRPDE.

Fondée et résolue

L'institution ou l'organisation a enfreint une disposition de la LPRP ou de la LPRPDE, mais elle a par la suite pris des mesures correctives pour remédier à la situation à la satisfaction du Commissariat.

Fondée et conditionnellement résolue

L'institution ou l'organisation a enfreint une disposition d'une loi sur la protection des renseignements personnels. L'institution ou l'organisation s'est engagée à mettre en œuvre des mesures correctives satisfaisantes approuvées par le Commissariat.

Non fondée

L'enquête n'a pas mis au jour des éléments de preuve suffisants pour conclure que l'institution ou l'organisation a enfreint une loi sur la protection des renseignements personnels.

Résolue

En vertu de la LPRP, l'enquête a révélé que la plainte découle essentiellement d'une mauvaise communication, d'un malentendu, etc., entre les parties, et/ou l'institution a accepté de prendre des mesures pour remédier à la situation à la satisfaction du Commissariat.

Réglée

Le Commissariat a aidé à négocier en cours d'enquête une solution satisfaisante pour toutes les parties en cause et n'a publié aucune conclusion.

Abandonnée

En vertu de la LPRP : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Diverses raisons peuvent entraîner l'abandon d'un dossier, mais ce ne peut être à la demande du Commissariat. Par exemple, il est possible que le plaignant ne veuille pas poursuivre la démarche ou que l'on ne puisse trouver ses coordonnées afin qu'il fournisse des renseignements supplémentaires essentiels pour en arriver à une conclusion.

En vertu de la LPRPDE : L'enquête a pris fin sans qu'une conclusion n'ait été publiée. Le commissaire peut mettre fin à l'enquête à sa discrétion pour un motif prévu au paragraphe 12.2(1) de la LPRPDE.

Hors du champ d'application

On a déterminé qu'aucune loi fédérale sur la protection des renseignements personnels ne s'applique à l'institution ou à l'organisation ou ne régit l'objet de la plainte. Par conséquent, le Commissariat ne produit aucun rapport.

Règlement rapide

La situation a été réglée à la satisfaction du plaignant dès le début du processus d'enquête. Le Commissariat n'a publié aucune conclusion.

Refus d'enquêter

En vertu de la LPRPDE, le commissaire a refusé d'amorcer l'examen d'une plainte, car il estime :

- que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement offerts;
- que la plainte pourrait avantageusement être instruite selon d'autres procédures prévues par le droit fédéral ou provincial ou;
- que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, comme le prévoit l'article 12(1) de la LPRPDE.

Retrait

En vertu de la LPRPDE, le plaignant a retiré sa plainte volontairement ou ne pouvait plus être joint dans les faits. Le Commissariat ne publie aucun rapport.

Annexe 2 :

Tableaux statistiques

Tableaux relatifs à la LPRP

Tableau 1

Décisions sur les plaintes* relatives à l'accès et à la protection des renseignements personnels en vertu de la LPRP, par institution fédérale

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Affaires mondiales Canada	1		1			1		5	8
Agence canadienne d'inspection des aliments								1	1
Agence de la santé publique du Canada			2					1	3
Agence des services frontaliers du Canada	6		9	1	1		4	19	40
Agence du revenu du Canada	1		9		1	3	2	28	44
Anciens combattants Canada	1		2	1				4	8
Bibliothèque et Archives Canada			1					1	2
Bureau de l'enquêteur correctionnel	2		1					1	4
Bureau du surintendant des institutions financières Canada			1						1
Comité de surveillance des activités de renseignement de sécurité								2	2
Commissariat à l'intégrité du secteur public du Canada			1						1
Commission canadienne des droits de la personne							1	2	3
Commission de l'assurance-emploi du Canada								1	1
Commission de la fonction publique du Canada			1			1		2	4
Commission des libérations conditionnelles du Canada					1			1	2
Commission des relations de travail et de l'emploi dans le secteur public fédéral								1	1

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Condition féminine Canada								2	2
Conseil canadien des relations industrielles								1	1
Conseil de la radiodiffusion et des télécommunications canadiennes			1					2	3
Conseil de recherches en sciences humaines du Canada			1						1
Construction de Défense Canada			1						1
Défense nationale			21	1	2		5	20	49
Élections Canada / Bureau du Directeur général des élections du Canada			1						1
Emploi et Développement social Canada	2		10	1		3		27	43
Énergie atomique du Canada limitée								1	1
Environnement et Changement climatique Canada								2	2
Gendarmerie royale du Canada	6		22	3	1	4	4	36	76
Immigration, Réfugiés et Citoyenneté Canada	1		9			4	1	21	36
Innovation, Sciences et Développement économique Canada						1		1	2
Ministère de la Justice Canada			2				3	4	9
Monnaie royale canadienne								2	2
Office des transports du Canada			1					2	3
Office national de l'énergie			1			1		1	3
Office national du film du Canada								1	1
Ombudsman de la Défense nationale et des Forces canadiennes			1						1
Pêches et Océans Canada			6			3	2	2	13
Relations Couronne-Autochtones et Affaires du Nord Canada		1	1					8	10
Santé Canada	1		2					7	10
Secrétariat du Conseil du Trésor du Canada			1					1	2
Sécurité publique Canada								2	2
Service Canada						2		1	3
Service canadien du renseignement de sécurité			5	1				12	18

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Service correctionnel Canada	5		15	3	1	5	4	50	83
Service des poursuites pénales du Canada							1		1
Services aux Autochtones Canada								2	2
Services partagés Canada								1	1
Services publics et Approvisionnement Canada			3				1	9	13
Société canadienne des postes			2			2	3	23	30
Société Radio-Canada			3					3	6
Statistique Canada			4					11	15
Technologies du développement durable du Canada			2				1		3
Transports Canada	1		2		1		2	7	13
VIA Rail Canada				1		1			2
Total	27	1	145	12	8	31	34	331	589

* Dossiers de plaintes en vertu de la LPRP fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 2

Délais de traitement des plaintes en vertu de la LPRP – Règlement rapide, par type de plainte*

Type de plainte	Nombre	Délai de traitement moyen en mois
Accès	175	3,48
Accès	167	3,32
Correction ou annotation	5	3,23
Langue	3	12,93
Délais	103	0,05
Correction ou annotation	1	0,01
Délais	102	0,05
Protection des renseignements personnels	155	5,29
Collecte	21	7,04
Conservation et retrait	6	2,68
Exactitude	3	0,90
Utilisation et communication	125	5,23
Total	433	3,31

* Dossiers de plaintes en vertu de la LPRP fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 3

Délais de traitement des plaintes en vertu de la LPRP – Enquêtes officielles, par type de plainte*

Type de plainte	Nombre	Délai de traitement moyen en mois
Accès	129	21,70
Accès	125	21,52
Correction ou annotation	3	22,42
Langue	1	42,41
Délais	674	6,98
Avis de prorogation	10	8,78
Correction ou annotation	1	0,75
Délais	663	6,96
Protection des renseignements personnels	130	27,54
Collecte	31	26,57
Conservation et retrait	8	24,56
Exactitude	4	14,01
Utilisation et communication	87	28,78
Total	933	11,88

* Dossiers de plaintes en vertu de la LPRP fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 4

Délais de traitement des plaintes en vertu de la LPRP – Tous les dossiers fermés, par décision*

Type de plainte	Nombre	Délai de traitement moyen en mois
Résolues par règlement rapide	433	3,31
Enquêtes officielles	933	11,88
Abandonnée	57	12,05
Fondée	49	20,70
Fondée et conditionnellement résolue	67	5,73
Fondée et résolue	577	8,23
Hors du champ d'application	1	42,66
Non fondée	160	22,74
Réglée	8	31,88
Résolue	14	22,45
Total	1 366	9,16

* Dossiers de plaintes en vertu de la LPRP fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 5

Atteintes en vertu de la LPRP, par institution

Intimé	Nombre
Affaires mondiales Canada	2
Agence des services frontaliers du Canada	2
Agence du revenu du Canada	6
Banque du Canada	1
Biens non publics et Personnel des fonds non publics, Forces canadiennes	1
Bureau de l'enquêteur correctionnel	3
Centre de la sécurité des télécommunications Canada	1
Commissariat à l'information du Canada	1
Commission de la fonction publique du Canada	4
Condition féminine Canada	1
Emploi et Développement social Canada	78
Environnement et Changement climatique Canada	1
Gendarmerie royale du Canada	11
Immigration, Réfugiés et Citoyenneté Canada	6
Innovation, Sciences et Développement économique Canada	1
Ministère des Finances Canada	1
Office national de l'énergie	1
Patrimoine canadien	2
Pêches et Océans Canada	1
Relations Couronne-Autochtones et Affaires du Nord Canada	1
Ressources naturelles Canada	1
Sécurité publique Canada	1
Service correctionnel Canada	10
Service des poursuites pénales du Canada	1
Services partagés Canada	3
Services publics et Approvisionnement Canada	4
Société canadienne des postes	2
Société Radio-Canada	1
Statistique Canada	6
Total	155

Tableau 6

Plaintes et atteintes en vertu de la LPRP

Catégorie	Total
Acceptées	
Accès	391
Délais	799
Protection des renseignements personnels	230
Total des plaintes acceptées*	1 420
Fermées à la suite d'un règlement rapide	
Accès	155
Délais	103
Protection des renseignements personnels	175
Total	433
Fermées à la suite d'une enquête officielle	
Accès	129
Délais	674
Protection des renseignements personnels	130
Total	933
Total des dossiers fermés**	1 366
Atteintes signalées	
Accès non autorisé	17
Communication accidentelle	61
Perte	69
Vol	8
Total des atteintes signalées	155

* Comprend une plainte représentative pour chacune de plusieurs séries de plaintes similaires, et pour des plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 95.

** Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 7

Plaintes en vertu de la LPRP acceptées, par type de plainte

Type de plainte	Règlement rapide		Enquête officielle		Nombre total	Pourcentage total*
	Nombre	Pourcentage*	Nombre	Pourcentage*		
Accès						
Accès	250	46 %	116	13 %	366	26 %
Correction ou annotation	18	3 %	6	1 %	24	2 %
Langue	1	0 %			1	0 %
Délais						
Avis de prorogation			12	1 %	12	1 %
Correction ou annotation	1	0 %	1	0 %	2	0 %
Délais	102	19 %	683	78 %	785	55 %
Protection des renseignements personnels						
Collecte	29	5 %	23	3 %	52	4 %
Conservation et retrait	10	2 %	2	0 %	12	1 %
Exactitude	4	1 %	1	0 %	5	0 %
Utilisation et communication	133	24 %	28	3 %	161	11 %
Total	548	100 %	872	100 %	1,420	100 %

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 8

Les 10 institutions fédérales visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP*

Intimé	Protection des renseignements personnels		Accès		Délais		Total
	Règlement rapide	Enquête officielle	Règlement rapide	Enquête officielle	Règlement rapide	Enquête officielle	
Service correctionnel Canada	20	4	31	14	11	346	426
Gendarmerie royale du Canada	23	6	27	13	14	190	273
Défense nationale	13	6	25	6	18	53	121
Agence des services frontaliers du Canada	13	7	31	23	6	29	109
Agence du revenu du Canada	21	4	19	12	6	17	79
Immigration, Réfugiés et Citoyenneté Canada	11	1	18	1	22	6	59
Emploi et Développement social Canada	13	1	15	6	2	2	39
Statistique Canada	4	10	7	1		12	34
Société canadienne des postes	10	1	13	1	2	2	29
Services publics et Approvisionnement Canada	5	1	9		7	5	27
Total	133	41	195	77	88	662	1 196

* Comprend une plainte représentative pour chacune de plusieurs séries de plaintes similaires, et pour des plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 95.

Tableau 9

Les 10 institutions fédérales visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP*, par exercice financier

Intimé	2015-2016	2016-2017	2017-2018	2018-2019
Service correctionnel Canada	547	389	440	426
Gendarmerie royale du Canada	120	160	232	273
Défense nationale	77	146	93	121
Agence des services frontaliers du Canada	88	107	76	109
Agence du revenu du Canada	85	65	63	79
Immigration, Réfugiés et Citoyenneté Canada	44	60	29	59
Emploi et Développement social Canada	42	36	24	39
Statistique Canada	5	22	4	34
Société canadienne des postes	17	19	33	29
Services publics et Approvisionnement Canada	10	25	49	27
Total	1 035	1 029	1 043	1 196

* Comprend une plainte représentative pour chacune de plusieurs séries de plaintes similaires, et pour des plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 95.

Tableau 10

Plaintes en vertu de la LPRP acceptées*, par institution

Intimé	Règlement rapide	Enquête officielle	Total
Affaires mondiales Canada	9	11	20
Agence canadienne de développement économique du Nord		1	1
Agence canadienne d'inspection des aliments	1	1	2
Agence de la santé publique du Canada	1		1
Agence des services frontaliers du Canada	50	59	109
Agence du revenu du Canada	46	33	79
Agence Parcs Canada	1	1	2
Anciens combattants Canada	16	4	20
Banque du Canada	1		1
Bibliothèque et Archives Canada	1		1
Biens non publics et Personnel des fonds non publics, Forces canadiennes	1		1
Bureau de l'enquêteur correctionnel	1	4	5
Centre de la sécurité des télécommunications Canada	1	2	3
Citoyenneté et Immigration Canada	1		1
Comité de surveillance des activités de renseignement de sécurité	2	2	4
Commission canadienne des droits de la personne		1	1
Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada		6	6
Commission de la fonction publique du Canada	4	1	5
Commission de l'assurance-emploi du Canada	1		1
Commission de l'immigration et du statut de réfugié du Canada	3		3
Commission des libérations conditionnelles du Canada	2	4	6

Intimé	Règlement rapide	Enquête officielle	Total
Commission des relations de travail et de l'emploi dans le secteur public fédéral	1		1
Conseil canadien des relations industrielles	1		1
Conseil de la radiodiffusion et des télécommunications canadiennes	2		2
Conseil de recherches en sciences humaines du Canada	4	3	7
Conseil de recherches en sciences naturelles et en génie du Canada	4	1	5
Conseil des arts du Canada	1		1
Défense nationale	56	65	121
École de la fonction publique du Canada		2	2
Emploi et Développement social Canada	30	9	39
Énergie atomique du Canada limitée	1	2	3
Environnement et Changement climatique Canada	4		4
Gendarmerie royale du Canada	64	209	273
Immigration, Réfugiés et Citoyenneté Canada	51	8	59
Innovation, Sciences et Développement économique Canada	1	1	2
Instituts de recherche en santé du Canada	1		1
Ministère de la Justice Canada	5	11	16
Monnaie royale canadienne	2		2
Office des transports du Canada	1		1
Office national de l'énergie		1	1
Ombudsman de la Défense nationale et des Forces canadiennes		1	1
Pêches et Océans Canada	5	3	8
Relations Couronne-Autochtones et Affaires du Nord Canada	9	1	10
Santé Canada	5	1	6
Secrétariat du Conseil du Trésor du Canada	2	1	3
Sécurité publique Canada	1	14	15
Service Canada	1		1
Service canadien d'appui aux tribunaux administratifs	1	2	3
Service canadien du renseignement de sécurité	19	5	24
Service correctionnel Canada	62	364	426
Service des poursuites pénales du Canada		2	2
Services aux Autochtones Canada	2	1	3
Services partagés Canada	1		1
Services publics et Approvisionnement Canada	21	6	27
Société canadienne des postes	25	4	29
Société Radio-Canada	2		2
Statistique Canada	11	23	34
Transports Canada	10	2	12
Total	548	872	1 420

* Comprend une plainte représentative pour chacune de plusieurs séries de plaintes similaires, et pour des plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 95.

Tableau 11
Plaintes en vertu de la LPRP acceptées, par province, territoire ou autres

	Règlement rapide		Enquête officielle		Nombre total	Pourcentage total*
Province, territoire ou autres	Nombre	Pourcentage*	Nombre	Pourcentage*		
Ontario	215	39,23 %	359	41,17 %	574	40,42 %
Québec	107	19,53 %	105	12,04 %	212	14,93 %
Nouvelle-Écosse	11	2,01 %	17	1,95 %	28	1,97 %
Nouveau-Brunswick	9	1,64 %	11	1,26 %	20	1,41 %
Manitoba	17	3,10 %	16	1,83 %	33	2,32 %
Colombie-Britannique	101	18,43 %	211	24,20 %	312	21,97 %
Île-du-Prince-Édouard	0	0,00 %	2	0,23 %	2	0,14 %
Saskatchewan	18	3,28 %	16	1,83 %	34	2,39 %
Alberta	44	8,03 %	111	12,73 %	155	10,92 %
Terre-Neuve-et-Labrador	7	1,28 %	13	1,49 %	20	1,41 %
Territoires du Nord-Ouest	2	0,36 %	0	0,00 %	2	0,14 %
Yukon	1	0,18 %	0	0,00 %	1	0,07 %
Nunavut	0	0,00 %	0	0,00 %	0	0,00 %
États-Unis	2	0,36 %	8	0,92 %	10	0,70 %
Autres (excluant les États-Unis)	3	0,55 %	1	0,11 %	4	0,28 %
Non précisé	11	2,01 %	2	0,23 %	13	0,92 %
Total	548	100,00 %	872	100,00 %	1 420	100,00 %

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 12
Décisions en vertu de la LPRP, par type de plainte*

Type de plainte	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Réglée rapidement	Total
Accès										
Accès	7		73	7	3	4		30	168	292
Correction ou annotation			2	1					5	8
Langue				1					3	4
Délais										
Avis de prorogation	1		3			4		2		10
Correction ou annotation								1	1	2
Délais	29		12	1		14	67	540	102	765
Protection des renseignements personnels										
Collecte	9		14		2	6			21	52
Conservation et retrait	1		6			1			6	14
Exactitude	1		1	1		1			3	7
Utilisation et communication	9	1	49	2	3	19		4	125	212
Total	57	1	160	13	8	49	67	577	434	1 366

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableau 13

Décisions sur les plaintes relatives aux délais en vertu de la LPRP*, par institution fédérale

Intimé	Abandonnée	Non fondée	Résolue	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Réglée rapidement	Total
Affaires mondiales Canada						1	2	3
Agence des services frontaliers du Canada					1	17	6	24
Agence du revenu du Canada	1					12	6	19
Anciens combattants Canada						1	7	8
Bureau de l'enquêteur correctionnel		1						1
Comité de surveillance des activités de renseignement de sécurité						1		1
Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada						1		1
Commission de la fonction publique du Canada		1						1
Conseil de recherches en sciences humaines du Canada		2						2
Défense nationale	2		1			57	18	78
Emploi et Développement social Canada						3	2	5
Gendarmerie royale du Canada	5	7		1		152	14	179
Immigration, Réfugiés et Citoyenneté Canada	1					7	22	30
Ministère de la Justice Canada						3		3
Relations Couronne-Autochtones et Affaires du Nord Canada							1	1
Santé Canada				2		1		3
Secrétariat du Conseil du Trésor du Canada							1	1
Service canadien du renseignement de sécurité		1				2	1	4
Service correctionnel Canada	9	1		12	66	272	11	371
Service des poursuites pénales du Canada						1		1
Services publics et Approvisionnement Canada				1		6	7	14
Société canadienne des postes		2		2		1	2	7
Statistique Canada	12							12
Transports Canada						5	3	8
Total	30	15	1	18	67	543	103	777

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 223.

Tableaux relatifs à la LPRPDE

Tableau 1

Plaintes en vertu de la LPRPDE acceptées*, par secteur de l'industrie

Secteur de l'industrie	Nombre	Proportion de l'ensemble des plaintes acceptées**
Aliments et boissons	5	1 %
Assurances	17	4 %
Construction	5	1 %
Divertissement	4	1 %
Édition (sauf Internet)	4	1 %
Fabrication	18	5 %
Finances	75	20 %
Gouvernement	1	0 %
Hébergement	36	9 %
Internet	37	10 %
Location	2	1 %
Organismes sans but lucratif	3	1 %
Personnes	1	0 %
Professionnels	11	3 %
Santé	2	1 %
Services	41	11 %
Services publics	3	1 %
Télécommunications	48	13 %
Transports	37	10 %
Ventes et détail	29	8 %
Non précisé	1	0 %
Total	380	100 %

* Plaintes en vertu de la LPRPDE acceptées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 100.

** Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 2

Plaintes en vertu de la LPRPDE acceptées*, par type de plainte

Type de plainte	Nombre	Proportion de l'ensemble des plaintes acceptées**
Accès	110	29 %
Collecte	49	13 %
Consentement	64	17 %
Conservation	10	3 %
Correction ou annotation	2	1 %
Détermination des fins	1	0 %
Exactitude	3	1 %
Fins acceptables	3	1 %
Mesures de sécurité	59	16 %
Possibilité de porter plainte	1	0 %
Responsabilité	8	2 %
Utilisation et communication	69	18 %
Autres	1	0 %
Total	380	100 %

* Plaintes en vertu de la LPRPDE acceptées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 100.

** Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 3

Dossiers d'enquête liés à la LPRPDE fermés*, par secteur de l'industrie et décision

Secteur de l'industrie	Réglée rapidement	Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Non fondée	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Retirée	Total
Aliments et boissons	3									1	4
Assurances	6	1	1	1	3				3		15
Construction	1										1
Divertissement	4							1			5
Édition (sauf Internet)	4							2			6
Fabrication	4								1		5
Finances	27		10		3		2	3	6	5	56
Gouvernement	1										1
Hébergement	13		1		1		1		2		18
Internet	24		3		1	1		1	2	4	36
Location	1										1
Organismes sans but lucratif			1								1
Professionnels	7		1	2	2		1		1		14
Santé			8	2						1	11

Secteur de l'industrie	Réglée rapidement	Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Non fondée	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Retirée	Total
Services	22			1		1		1	1		26
Services publics	1		1								2
Télécommunications	31		2		1			2	1	2	39
Transports	11		4						2	1	18
Ventes et détail	17		1						2	1	21
Non spécifié	1						1				2
Total	178	1	33	6	11	2	5	10	21	15	282

* Dossiers d'enquête en vertu de la LPRPDE fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 110.

Tableau 4

Dossiers d'enquête liés à la LPRPDE fermés*, par type de plainte et décision

Type de plainte	Réglée rapidement	Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Non fondée	Réglée	Fondée	Fondée et conditionnellement résolue	Fondée et résolue	Retirée	Total
Accès	46		13	3	2		1	3	12	4	84
Collecte	26				1	1		2	2	2	34
Consentement	32	1	7	1	3	1	2	4		8	59
Conservation	8										8
Correction ou annotation	2									1	3
Détermination des fins					1						1
Exactitude	2		1		1						4
Fins acceptables	1		1								2
Mesures de sécurité	16		4		1				3		24
Responsabilité	2		2		1						5
Utilisation et communication	43		5	2	1		2	1	3		57
Autre									1		1
Total	178	1	33	6	11	2	5	10	21	15	282

* Dossiers d'enquête en vertu de la LPRPDE fermés en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 110.

Tableau 5

Enquêtes en vertu de la LPRPDE* – Délais de traitement moyens, par décision

Décision	Nombre	Délai de traitement moyen, en mois
Abandonnée (article 12.2)	33	9,5
Fondée	5	20,3
Fondée et conditionnellement résolue	10	22,4
Fondée et résolue	21	15,9
Hors du champ d'application	6	10,8
Non fondée	11	16,8
Refusée	1	6,7
Réglée	2	14,6
Résolue par règlement rapide	178	2,7
Retirée	15	20,2
Total	282	
Moyenne générale pondérée		7,3

* Enquêtes en vertu de la LPRPDE en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 110.

Tableau 6

Enquêtes en vertu de la LPRPDE* – Délais de traitement moyens, par type de plainte et de règlement

	Règlement rapide		Autres règlements		Toutes les enquêtes	
Type de plainte	Nombre	Délai de traitement moyen en mois	Nombre	Délai de traitement moyen en mois	Nombre	Délai de traitement moyen en mois
Accès	46	3,1	38	14,3	84	8,2
Collecte	26	2,0	8	22,3	34	6,8
Consentement	32	2,8	27	16,6	59	9,1
Conservation	8	2,3			8	2,3
Correction ou annotation	2	0,9	1	15,3	3	5,7
Détermination des fins			1	10,2	1	10,2
Exactitude	2	4,0	2	19,6	4	11,8
Fins acceptables	1	2,0	1	17,6	2	9,8
Mesures de sécurité	16	2,4	8	20,6	24	8,4
Responsabilité	2	2,6	3	3,1	5	2,9
Utilisation et communication	43	3,0	14	8,7	57	4,4
Autres			1	14,6	1	14,6
Total	178	2,7	104	15,0	282	7,3

* Enquêtes en vertu de la LPRPDE en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 110.

Tableau 7

Déclarations des atteintes en vertu de la LPRPDE, par secteur de l'industrie et type d'incident

Secteur	Type d'incident					Proportion de l'ensemble des incidents*
	Communication accidentelle	Perte	Vol	Accès non autorisé	Total des incidents par secteur	
Aliments et boissons		1			1	0 %
Assurances	12	1	6	5	24	8 %
Construction	2				2	1 %
Divertissement			1	3	4	1 %
Édition	1		1	6	8	3 %
Extraction minière et extraction de pétrole et de gaz	1			1	2	1 %
Fabrication	2			10	12	4 %
Finances	20	3	9	38	70	22 %
Gouvernement	1		1	1	3	1 %
Hébergement				5	5	2 %
Internet	5		1	8	14	4 %
Organismes sans but lucratif	8	1	1	4	14	4 %
Professionnels	3	1	2	6	12	4 %
Santé	7	1	1	3	12	4 %
Services	2			15	17	5 %
Services publics				1	1	0 %
Télécommunications	6		3	43	52	17 %
Transports	1			3	4	1 %
Ventes et détail	11	19	1	26	57	18 %
Non précisé	1				1	0 %
Total	83	27	27	178	315	100 %

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Annexe 3 : Processus d'enquête

PROCESSUS D'ENQUÊTE EN VERTU DE LA LPRP

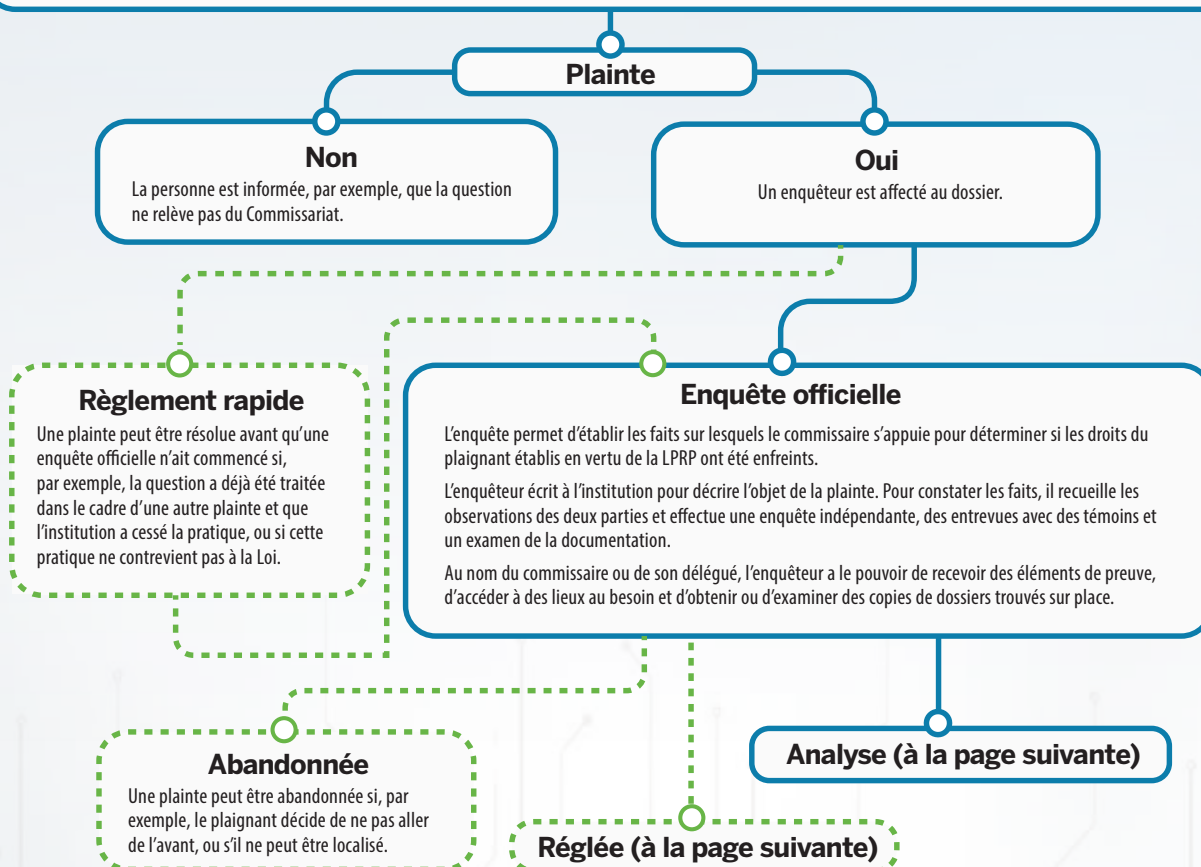
Accueil

Des personnes font parvenir des plaintes écrites au Commissariat concernant des infractions à la LPRP. L'unité d'accueil examine l'affaire en cause afin de déterminer si elle constitue bel et bien une plainte, selon que les faits allégués pourraient contrevenir ou non à la Loi, ainsi que le moyen le plus efficace de la résoudre.

Une personne peut déposer une plainte se rapportant à toute question énoncée à l'article 29 de la LPRP – par exemple :

- le refus d'une institution de communiquer à une personne les renseignements personnels qu'elle détient à son sujet, ou un retard inacceptable dans la communication de ces renseignements;
- la collecte, l'utilisation ou la communication inappropriée de renseignements personnels;
- des erreurs dans les renseignements personnels qu'une institution utilise ou communique.

L'unité d'accueil réussit parfois à régler immédiatement les problèmes, éliminant ainsi la nécessité pour le Commissariat de s'occuper du dossier dans le cadre d'une enquête officielle. Dans ces cas, le Commissariat ferme simplement le dossier, et la plainte est considérée comme ayant été réglée rapidement. Le commissaire à la protection de la vie privée peut lui aussi déposer une plainte s'il est d'avis qu'il y a des motifs suffisants pour mener une enquête.



Nota : Une ligne discontinue (- - -) indique un résultat possible.

Enquête officielle

(suite de la page précédente)

Analyse

L'enquêteur analyse les faits et prépare les recommandations pour le commissaire ou son délégué. Il communique avec les parties, au besoin, et examine les faits recueillis au cours de l'enquête. Il peut également informer les parties des recommandations, fondées sur les faits, qu'il présentera au commissaire ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.

Au besoin, des consultations internes sont effectuées avec, par exemple, la Direction des services juridiques, la Direction des politiques, de la recherche et des affaires parlementaires ainsi que la Direction de l'analyse de la technologie.

Conclusion

Le commissaire ou son délégué examine le dossier et évalue le rapport. Le commissaire ou son délégué, et non l'enquêteur, décide de l'issue appropriée du dossier et s'il faut présenter des recommandations à l'institution.

Le commissaire ou son délégué envoie aux parties des lettres de conclusions décrivant le motif de la plainte, les conclusions de faits dignes d'intérêt, l'analyse et les recommandations à l'institution. Le commissaire ou son délégué peut demander à l'institution de lui indiquer par écrit, dans un délai précis, les mesures prévues pour mettre en œuvre les recommandations.

Les conclusions possibles au sujet de la plainte sont les suivantes :

Non fondée : La preuve, tout bien pesé, ne permet pas au commissaire ou à son délégué de conclure que les droits du plaignant en vertu de la Loi ont été enfreints.

Fondée : L'institution n'a pas respecté l'une des dispositions de la Loi.

Fondée et résolue : Les allégations sont corroborées par l'enquête et l'institution a accepté de prendre des mesures correctives afin de remédier à la situation.

Résolue : La preuve recueillie au cours de l'enquête soutient les allégations formulées dans la plainte, mais l'institution s'est engagée à prendre des mesures pour remédier à la situation à la satisfaction du Commissariat. Cette conclusion est réservée aux plaintes qu'on pourrait difficilement qualifier de fondées du fait que la situation relève essentiellement d'une mauvaise communication ou d'un malentendu.

Dans sa lettre de conclusions, le commissaire ou son délégué informe le plaignant de son droit de recours à la Cour fédérale pour les cas de refus d'accès aux renseignements personnels.

Réglée

Le Commissariat cherche à régler les plaintes et à prévenir d'autres infractions à la Loi. Le commissaire favorise la résolution des différends par l'entremise de la négociation et de la persuasion. L'enquêteur participe au processus.

Lorsque des recommandations ont été présentées à une institution, le personnel du Commissariat effectue un suivi pour vérifier si elles ont bel et bien été appliquées.

En cas de refus d'accès aux renseignements personnels, le plaignant ou le commissaire peut choisir de demander une audience à la Cour fédérale. La Cour fédérale a le pouvoir d'examiner l'affaire et de déterminer si l'institution doit fournir les renseignements au requérant.

Nota : Une ligne discontinue (- - - -) indique un résultat possible.

PROCESSUS D'ENQUÊTE EN VERTU DE LA LPRPDE

Accueil

Des personnes font parvenir des plaintes écrites au Commissariat concernant des infractions à la Loi. L'unité d'accueil examine les plaintes et effectue un suivi auprès des plaignants pour demander des précisions et recueillir des renseignements supplémentaires, le cas échéant.

Si les plaignants n'ont pas discuté de leurs préoccupations directement avec l'organisation visée, le Commissariat leur demande de le faire pour tenter de régler la question, puis de revenir le voir si leur démarche est infructueuse.

L'unité d'accueil réussit parfois à régler immédiatement les problèmes. Par exemple, si le Commissariat a déjà effectué une enquête sur le type de question soulevée et qu'il a jugé les activités conformes à la LPRPDE, un agent de réception des plaintes en informe la personne en cause. Par ailleurs, si le Commissariat a déterminé antérieurement qu'une organisation ou une activité n'est pas de son ressort, un agent de réception explique la situation et aiguille la personne vers d'autres ressources ou sources d'aide, s'il y a lieu.

Dans les cas où l'unité d'accueil n'est pas en mesure de régler immédiatement la question soulevée (et après que l'information nécessaire a été recueillie), le Commissariat considère qu'il s'agit d'une plainte officielle. Le commissaire à la protection de la vie privée peut lui aussi déposer une plainte s'il est d'avis qu'il y a des motifs suffisants pour mener une enquête.

Plainte refusée

Le commissaire peut refuser d'enquêter sur une plainte si certaines conditions prévues au paragraphe 12(1) de la Loi sont respectées. Le plaignant peut demander au commissaire de revenir sur sa décision.

Plainte confiée à un enquêteur

Les plaintes de nature grave, systémique ou complexe – par exemple, questions de compétence, allégations multiples ou aspects techniques complexes – sont confiées à un enquêteur.

Confiée à un agent de règlement rapide

Les plaintes qui, selon le Commissariat, peuvent être résolues rapidement sont confiées à un agent de règlement rapide. Il s'agit de plaintes sur des sujets ayant déjà fait l'objet de conclusions de la part du Commissariat, qui concernent des organisations ayant déjà répondu aux allégations de façon satisfaisante aux yeux du Commissariat ou encore de cas où il semble possible de régler rapidement les allégations.

Enquête

Les enquêtes établissent les faits permettant au commissaire de déterminer si les droits du plaignant ont été enfreints au sens de la LPRPDE.

L'enquêteur écrit à l'organisation pour décrire l'objet de la plainte. Pour constater les faits, il recueille les observations des deux parties et effectue une enquête indépendante, des entrevues avec des témoins et un examen de la documentation. Au nom du commissaire ou de son délégué, l'enquêteur a le pouvoir de recevoir des éléments de preuve, d'accéder à des lieux au besoin et d'obtenir ou d'examiner des copies de dossiers trouvés sur place.

Acheminée à un enquêteur

Une plainte qui ne peut être réglée rapidement est confiée à un enquêteur.

Réglée rapidement

Des agents de règlement rapide favorisent le règlement des plaintes au moyen de la médiation, de la négociation et de la persuasion.

Abandonnée

Une plainte peut être abandonnée, par exemple, si le plaignant décide de ne pas aller de l'avant ou s'il ne peut être localisé, ou encore si certaines conditions prévues à l'article 12.2 de la Loi sont respectées.

Analyse (à la page suivante)

Réglée (à la page suivante)

Enquête officielle

(suite de la page précédente)

Analyse

L'enquêteur analyse les faits et prépare les recommandations pour le commissaire ou son délégué.

Il communique avec les parties et examine les faits recueillis au cours de l'enquête. Il informe également les parties des recommandations, fondées sur les faits, qu'il présentera au commissaire ou à son délégué. À cette étape, les parties peuvent faire d'autres observations.

Au besoin, des consultations internes sont effectuées avec, par exemple, la Direction des services juridiques, la Direction des politiques, de la recherche et des affaires parlementaires ainsi que la Direction de l'analyse de la technologie.

Réglée

Le Commissariat cherche à régler les plaintes et à prévenir d'autres infractions à la Loi. Il aide à négocier, en cours d'enquête, une solution qui convient à toutes les parties. L'enquêteur participe au processus.

Hors du champ d'application

Le Commissariat détermine que la LPRPDE ne s'applique pas à l'organisation en cause ou aux activités faisant l'objet de la plainte.

Conclusions

Le commissaire ou son délégué examine le dossier et évalue le rapport. Le commissaire ou son délégué, et non l'enquêteur, décide de l'issue appropriée du dossier et s'il faut présenter des recommandations à l'organisation.

Rapport préliminaire

Si l'enquête laisse croire qu'il y a vraisemblablement eu une infraction à la LPRPDE, le commissaire ou son délégué fait des recommandations pour aider l'organisation à régler le problème et demande à celle-ci de préciser dans un délai fixé comment elle appliquera les recommandations.

Rapport final et lettres de conclusions

Le commissaire ou son délégué envoie aux parties des lettres de conclusions décrivant le motif de la plainte, les conclusions de faits dignes d'intérêt, l'analyse et la réponse de l'organisation à toute recommandation formulée dans le rapport préliminaire.

(Les conclusions possibles sont indiquées à l'annexe 1 – Définitions.)

Dans sa lettre de conclusions, le commissaire ou son délégué informe le plaignant de son droit de recours à la Cour fédérale.

Si certaines recommandations n'ont pas encore été mises en œuvre par l'organisation, le Commissariat lui demande de le tenir au courant de la situation, selon un calendrier prédéterminé après l'enquête, afin qu'il puisse évaluer si des mesures correctives ont été prises.

Le plaignant ou le commissaire peut choisir de demander une audience à la Cour fédérale. Celle-ci a le pouvoir d'ordonner à l'organisation de revoir ses pratiques. Elle peut également accorder des dommages-intérêts au plaignant, notamment pour une humiliation subie. Le montant des dommages-intérêts n'est assujéti à aucune limite.

Annexe 4 :

Lois essentiellement similaires

En vertu du paragraphe 25(1) de la LPRPDE, le Commissariat doit déposer chaque année au Parlement un rapport « sur la mesure dans laquelle les provinces ont édicté des lois essentiellement similaires ».

En vertu de l'alinéa 26(2)b) de la LPRPDE, le gouverneur en conseil peut, par décret, exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de cette loi à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur d'une province ayant adopté une loi provinciale « essentiellement similaire ».

Le 3 août 2002, Industrie Canada (maintenant connu sous le nom d'Innovation, Sciences et Développement économique Canada) a publié le [Processus de détermination du caractère « essentiellement similaire » d'une loi provinciale](#) par le gouverneur en conseil. On y présente la politique et les critères utilisés pour déterminer si une loi provinciale sera considérée comme essentiellement similaire. En vertu de la politique, les lois essentiellement similaires :

- fournissent un mécanisme de protection des renseignements personnels conforme et équivalent à celui de la LPRPDE;
- intègrent les 10 principes de l'annexe 1 de la LPRPDE;
- fournissent un mécanisme indépendant et efficace de surveillance et de recours ainsi que des pouvoirs d'enquête;
- restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes.

Les organisations assujetties aux lois provinciales réputées essentiellement similaires sont exemptées de la LPRPDE en ce qui a trait à la collecte, à l'utilisation et à la communication de renseignements personnels à l'intérieur de la province visée. La LPRPDE continue toutefois de s'appliquer à la collecte, à l'utilisation ou à la communication de renseignements personnels liée aux activités d'entreprises fédérales dans la province visée ainsi qu'à la collecte, à l'utilisation ou à la communication de renseignements personnels à l'extérieur de cette province.

Les lois provinciales considérées comme essentiellement similaires sont les suivantes :

- *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec;
- *Personal Information Protection Act* de la Colombie-Britannique;
- *Personal Information Protection Act* de l'Alberta;
- *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario (dépositaires de renseignements sur la santé);
- *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* du Nouveau-Brunswick (dépositaires de renseignements sur la santé);
- *Personal Health Information Act* de Terre-Neuve-et-Labrador (dépositaires de renseignements sur la santé);
- *Personal Health Information Act* de la Nouvelle-Écosse (dépositaires de renseignements sur la santé).

Annexe 5 : Rapport de la commissaire spéciale à la protection de la vie privée



La commissaire spéciale à la protection de la vie privée enquête sur les plaintes concernant la manière dont le Commissariat à la protection de la vie privée traite les demandes d'accès aux renseignements personnels qu'il reçoit. Cette fonction a été créée car le Commissariat ne peut pas enquêter sur lui-même dans de tels cas.

Je suis devenue commissaire spéciale à la protection de la vie privée en avril 2018 et, à ce titre, je détiens les mêmes pouvoirs que le commissaire en ce qui a trait aux enquêtes et je peux formuler des recommandations quant à la façon de régler les plaintes que je reçois. Avant d'occuper ce poste, j'ai assumé les fonctions de commissaire à l'accès à l'information et à la protection de la vie privée du Nouveau-Brunswick de 2010 à 2017. J'ai également été commissaire aux conflits d'intérêts par intérim pour le Nouveau-Brunswick pendant un an (2015-2016). Auparavant, j'ai fait carrière comme avocate généraliste durant 24 ans et j'ai eu l'occasion de comparaître devant toutes les instances judiciaires, y compris la Cour suprême du Canada.

En 2018-2019, une plainte concernant le Commissariat à la protection de la vie privée a débouché sur la conclusion que, même si la demanderesse (plaignante) avait eu accès à tous les renseignements personnels auxquels elle avait droit, il est ressorti du dossier que de meilleures explications auraient pu être fournies à la demanderesse dès le début. Il n'a pas été nécessaire de formuler une recommandation dans ce cas-ci. Une autre affaire a donné lieu à un examen approfondi, mais n'a rien révélé qui puisse constituer une plainte recevable. Le reste du travail que j'ai reçu comprenait de la correspondance provenant de personnes qui n'étaient pas satisfaites de la façon dont le Commissariat traitait leurs dossiers, mais l'objet de ces derniers n'était pas de mon ressort. J'ai envoyé des lettres à ces personnes en leur fournissant ces explications.

La commissaire spéciale à la protection de la vie privée,

Anne E. Bertrand, c.r.