Commissariat
à la protection de
la vie privée du Canada

Rapport annuel au Parlement 2016–2017

concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*

DES CRAINTES RÉELLES, **DES SOLUTIONS POUR Y REMÉDIER**

Plan pour rétablir la confiance dans la protection de la vie privée

Rapport annuel au Parlement 2016-2017 concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*

Des craintes réelles, des solutions pour y remédier :
Plan pour rétablir la confiance dans la protection de la vie privée

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

Numéro de catalogue : IP51-1F-PDF
Numéro ISSN : 1913-3367

Suivez-nous sur Twitter : @PriveePrivacy
Facebook : https://www.facebook.com/ViePriveeCanada/

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (819) 994-5444
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
1-800-282-1376
www.priv.gc.ca

L'honorable George J. Furey, sénateur
Président
Sénat du Canada
Ottawa (Ontario)
K1A 0A4

Septembre 2017

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels* pour la période allant du 1er avril 2016 au 31 mars 2017.

Je vous prie d'agréer, Monsieur le Président, l'assurance de ma considération distinguée.

Original signé par

Le commissaire à la protection de la vie privée du Canada,

Daniel Therrien

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (819) 994-5444
1-800-282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
1-800-282-1376
www.priv.gc.ca

L'honorable Geoff Regan, C.P., député
Président
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Septembre 2017

Monsieur le Président,

J'ai l'honneur de présenter au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels* pour la période allant du 1er avril 2016 au 31 mars 2017.

Je vous prie d'agréer, Monsieur le Président, l'assurance de ma considération distinguée.

Original signé par

Le commissaire à la protection de la vie privée du Canada,

Daniel Therrien

Table des matières

Message du commissaire

La révolution numérique, que plusieurs qualifient de quatrième révolution industrielle, a apporté d'importants avantages aux individus—facilité de communication et accessibilité accrue à des renseignements, à des produits et à des services qui améliorent notre vie sur le plan matériel et intellectuel. Elle contribue grandement à la croissance économique et continuera de le faire. Toutefois, elle suscite aussi de grandes préoccupations. La crainte de perdre son emploi constitue sans doute la principale de ces préoccupations. Mais il y a aussi la crainte de violations importantes de notre vie privée et, par le fait même, la perte de notre droit inhérent à vivre et à nous épanouir en tant qu'êtres humains autonomes. Les sondages montrent de façon constante qu'une très grande majorité de Canadiens (plus de 90 %) ont des craintes au sujet de leur vie privée.

Le développement de la technologie, qui est une bonne chose dans l'ensemble, ne se fera pas de manière durable à moins que des solutions concrètes et substantielles n'apaisent les craintes des citoyens. Lors de nos consultations, les Canadiens nous ont dit, en ce qui concerne la protection de la vie privée, qu'ils souhaitent une meilleure information pour exercer un contrôle sur leurs propres renseignements personnels, mais ils s'attendent aussi à ce que le gouvernement assure une meilleure protection à cet égard. En effet, ils estiment que le gouvernement dispose de connaissances et d'outils plus appropriés pour assurer la protection de la vie privée.

Je suis d'accord avec les Canadiens. D'après moi, les solutions nécessaires pour répondre à leurs préoccupations devraient, bien entendu, comprendre une meilleure information pour leur donner le moyen d'exercer un contrôle et une autonomie personnels. Mais cela ne suffit pas. L'individu doit demeurer au centre de la protection de la vie privée mais des mécanismes de soutien plus forts sont aussi nécessaires—entre autres des organismes de réglementation indépendants, comme le Commissariat à la protection de la vie privée du Canada, disposant de ressources et de pouvoirs appropriés qui leur donnent une capacité réelle de guider l'industrie et de l'obliger à rendre des comptes, de renseigner les citoyens et d'imposer des sanctions efficaces en cas de conduite inappropriée.

Sur ce, j'ai le plaisir de présenter le Rapport annuel au Parlement 2016-2017 du Commissariat. Ce rapport porte à la fois sur la *Loi sur la protection des renseignements personnels,* qui s'applique aux pratiques de traitement des renseignements personnels des ministères et organismes fédéraux, et sur la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE),

la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada.

Comme c'était le cas lorsque j'ai déposé mon dernier rapport annuel, l'évolution rapide de la technologie—les mégadonnées, l'Internet des objets, la biométrie et l'intelligence artificielle, entre autres innovations—continue d'avoir une énorme incidence sur la protection des renseignements personnels. Les individus ont de plus en plus de difficulté à bien comprendre comment et à quelles fins les organisations recueillent, utilisent et communiquent leurs renseignements personnels, et encore plus à exercer un contrôle à cet égard.

Le Commissariat étudie attentivement ce phénomène et constate que la nécessité de moderniser notre régime de protection de la vie privée n'a jamais été plus manifeste ou urgente.

Les lois canadiennes sont neutres sur le plan technologique, mais leur adoption remonte à une époque très différente où les interactions individuelles courantes, prévisibles et transparentes entre les organisations et les individus constituaient la norme. Ce n'est plus le cas maintenant que les algorithmes informatiques et les immenses bases de données sont le moteur de l'économie et ouvrent la porte à de nouvelles possibilités attrayantes pour les institutions fédérales et les organisations du secteur privé. D'après notre dernier sondage d'opinion publique, dont les résultats ont été publiés en janvier, 92 % des Canadiens se préoccupent de la protection de leurs renseignements personnels et une nette majorité (57 %) était très inquiète.

Il y a certainement de quoi s'inquiéter. Certaines choses doivent changer, sans quoi nous courons le risque que les Canadiens perdent confiance dans l'économie numérique, ce qui entraverait sa croissance et les empêcherait de bénéficier de tous les avantages de l'innovation. Plus important encore, dans une société démocratique, il est très malsain que la plupart des citoyens craignent que l'un de leurs droits les plus fondamentaux ne soit pas respecté.

Au cours de la dernière année, nous avons pris plusieurs mesures concrètes pour remédier à ce problème. Nous avons formulé des recommandations concernant la réforme de la *Loi sur la protection des renseignements personnels,* le cadre de sécurité nationale du Canada et, dans le présent rapport, le rôle du consentement sous le régime de la législation fédérale sur la protection des renseignements personnels dans le secteur privé. En plus d'expliquer en détail ces travaux, ce rapport trace une nouvelle voie pour l'avenir de la protection de la vie privée au Canada.

Consultation sur le consentement et réforme de la LPRPDE

Le consentement est depuis longtemps considéré comme un élément de base de la LPRPDE. Il s'agit du principal mécanisme par lequel les individus peuvent affirmer leur autonomie et exercer un contrôle sur leurs renseignements personnels. En vertu de la loi, les organisations doivent obtenir le consentement d'un individu avant de recueillir, d'utiliser ou de communiquer ses renseignements personnels, sous réserve d'une liste d'exceptions très précises. Il est de plus en plus difficile d'obtenir un consentement valable à l'ère numérique, où les données deviennent omniprésentes, servent désormais de monnaie d'échange et peuvent être traitées par plusieurs intervenants tout à fait à l'insu de l'intéressé.

C'est pourquoi le Commissariat a publié en mai 2016 un document de discussion explorant l'applicabilité du modèle de consentement actuel sous le régime de la LPRPDE, la question de savoir si des changements s'imposent et qui devrait être responsable de quels changements—les organisations, les individus, les organismes de réglementation ou les législateurs.

Nous avons reçu plus de 50 mémoires d'entreprises, d'organisations de la société civile, d'universitaires,

d'avocats, de représentants d'organismes de réglementation et de citoyens. Nous avons aussi tenu cinq tables rondes réunissant des intervenants dans toutes les régions du Canada ainsi qu'une série de discussions de groupe auxquelles ont participé des Canadiens dans quatre villes. Après avoir consacré plusieurs mois à l'analyse de l'information ainsi recueillie, nous vous présentons avec plaisir nos conclusions dans le présent rapport annuel.

Pour commencer, on nous a dit à quel point les individus se sentent impuissants dans le marché numérique lorsqu'il s'agit d'exercer un contrôle sur la collecte et l'utilisation de leurs renseignements personnels par les entreprises. Les clients s'y perdent dans les politiques de confidentialité incompréhensibles et, pourtant, ils se sentent contraints d'accorder leur consentement pour obtenir les biens ou les services souhaités. Certains membres des groupes de discussion ont même affirmé que l'information fournie ne leur permet « jamais » vraiment de donner leur consentement en toute connaissance de cause.

Pourtant, la majorité des personnes et des organisations qui se sont exprimées s'entendaient pour dire que le consentement devrait continuer de jouer un rôle important dans la protection de la vie privée. Après de longues délibérations, nous avons présenté plusieurs mesures et recommandations visant à donner au consentement un caractère plus valable, mais aussi à renforcer le rôle des organisations et des organismes de réglementation parce que le consentement n'est pas toujours suffisant en tant qu'outil de protection de la vie privée. Nous avons proposé des solutions de remplacement pour les cas où les pratiques axées sur les données pourraient rendre le consentement inapplicable.

Par exemple, pour donner tout son sens au consentement, nous mettrons à jour nos lignes directrices en matière de consentement en ligne afin de préciser quatre éléments clés qui doivent être mis en évidence dans les avis de confidentialité et expliqués de manière conviviale. Nous informerons aussi les individus des outils de consentement existants et des autres technologies renforçant la protection de la vie privée qui peuvent les aider à faire respecter leurs préférences. Nous rédigerons à l'intention des entreprises un nouveau document d'orientation sur les zones interdites où l'utilisation des renseignements personnels, même avec le consentement de l'intéressé, devrait être prohibée en raison de son caractère inapproprié.

Nous avons conclu que l'on ne devrait pas s'attendre à ce que les individus aient le fardeau le plus lourd lorsqu'il s'agit de déconstruire des flux de données complexes pour prendre en toute connaissance de cause la décision de donner ou non leur consentement.

Les organisations doivent aussi faire preuve d'une transparence et d'une responsabilité accrues concernant leurs pratiques de protection de la vie privée. Puisqu'elles connaissent mieux que quiconque leurs activités, on est en droit de s'attendre à ce qu'elles trouvent des moyens efficaces dans leur contexte afin de protéger la vie privée de leurs clients, notamment en intégrant la protection de la vie privée dès la conception d'un programme. Au cours de nos enquêtes, nous continuerons de demander aux organisations de faire la preuve qu'elles respectent le principe de responsabilité prévu dans la LPRPDE et nous demanderons au Parlement de renforcer nos pouvoirs pour le faire appliquer de façon proactive. En outre, nous adapterons notre cadre de responsabilité actuel aux besoins des petites et moyennes entreprises.

Entre-temps, les organismes de réglementation, comme le Commissariat, sont bien placés pour jouer un rôle de premier plan au chapitre de l'éducation et de l'orientation. Dans le cadre de nos consultations, les participants nous ont constamment demandé de donner davantage d'orientation aux individus sur la façon d'exercer leur droit à la vie privée et aux

organisations sur la façon de s'acquitter de leurs obligations.

Ces commentaires nous ont incités à concentrer davantage nos efforts sur les citoyens. Nous avons déjà remanié notre site Web pour faciliter la navigation. En outre, nous élaborons actuellement de nouvelles fiches de conseils et de nouveaux documents d'orientation qui, nous l'espérons, sont plus faciles à comprendre et contiennent des conseils pratiques pour les citoyens et les organisations.

Nous continuerons de publier des orientations sur le plus grand nombre possible d'enjeux liés à la protection de la vie privée et aiderons l'industrie à élaborer des codes de pratique. Dans un premier temps, nous réviserons nos lignes directrices en matière de consentement en ligne, mais notre objectif consiste à fournir de l'information concernant une trentaine de sujets sur une période de quatre ans. Nous voulons que l'on nous évalue en fonction de l'utilité des orientations que nous donnons pour les individus et les organisations.

En ce qui a trait à l'éducation du public, la stratégie la plus efficace pourrait bien être de sensibiliser les enfants à la protection de la vie privée dès leur jeune âge. Nous exhortons donc les gouvernements provinciaux et territoriaux à intégrer ce sujet plus concrètement dans le programme d'études.

Nous reconnaissons qu'il faut encourager l'innovation et que les renseignements personnels constituent un volet important de l'économie axée sur les données. Toutefois, à certains égards, la complexité de la technologie et les modes d'utilisation des renseignements personnels et leurs conséquences peuvent rendre très difficile l'obtention d'un consentement valable. Pour prendre en compte ces réalités, nous publierons un document d'orientations sur les façons de dépersonnaliser les renseignements d'une manière conforme au respect de la vie privée. Nous encourageons le Parlement à faire suite à la recommandation d'intervenants du secteur privé et de se pencher sur la définition des « renseignements auxquels le public a accès », pour lesquels le consentement n'est pas nécessaire, et à déterminer s'il pourrait être approprié de prévoir de nouvelles exceptions à l'obligation d'obtenir un consentement lorsque ce n'est simplement ou pratiquement pas possible.

L'indexation des sites Web fait par les moteurs de recherche et l'analyse des mégadonnées ne sont que deux exemples où la quantité de renseignements recueillis et utilisés, ainsi que la rapidité de leur collecte et de leur utilisation peuvent rendre le consentement pratiquement impossible. Quelques représentants de l'industrie ont recommandé l'adoption au Canada du concept des « intérêts légitimes », qui est reconnu en droit européen comme motif pour le traitement de données. Il s'agit effectivement d'une option que le Parlement pourrait envisager mais, selon nous, cette exception à l'obligation d'obtenir le consentement serait très large. Si de nouvelles exceptions au consentement devaient être adoptées, nous pensons qu'il serait préférable qu'elles soient définies d'une façon plus ciblée. Nous pensons également qu'elles devraient être assujetties à des conditions rigoureuses et ne s'appliquer que dans les cas où les avantages pour la société—et non simplement ceux pour l'organisation—l'emportent manifestement sur l'ingérence dans la vie privée.

Enfin, le rôle des législateurs sera crucial pour s'assurer que les lois canadiennes sur la protection des renseignements personnels demeurent à jour et continuent de protéger efficacement les Canadiens contre le risque de préjudice.

Le moment est venu pour le Canada de modifier son modèle de protection de la vie privée afin de s'assurer que, tout comme aux États-Unis, au sein de l'Union européenne et ailleurs, ses organismes de réglementation peuvent protéger efficacement le droit à la vie privée de ses citoyens en ayant des pouvoirs

proportionnels au risque croissant d'atteinte à la vie privée que présentent les nouvelles technologies révolutionnaires.

Les Canadiens nous ont fait part de leurs inquiétudes. Les participants aux discussions de groupe sont généralement favorables à l'idée que le gouvernement contrôle les entreprises pour s'assurer qu'elles respectent les lois sur la protection des renseignements personnels. Ils conviennent que l'application de la loi doit se faire à la fois de façon proactive et réactive. Leur opinion reflète en grande partie les résultats du dernier sondage d'opinion publique réalisé par le Commissariat dans lequel sept répondants sur dix se sont dits favorables à ce que la loi confère au commissaire à la protection de la vie privée le pouvoir de rendre des ordonnances et la possibilité d'imposer des sanctions financières importantes aux organisations qui utilisent à mauvais escient leurs renseignements personnels.

En conséquence, nous proposons un modèle mettant l'accent sur une application de la loi proactive, assorti de pouvoirs d'ordonnance et de sanctions administratives pécuniaires. Le modèle devrait en outre expliciter l'obligation pour les organisations de démontrer leur respect du principe de la responsabilité.

Le modèle canadien de protection de la vie privée, principalement réactif et axé sur les plaintes, a obtenu un certain succès au fil des ans, mais il se heurte à d'énormes défis à l'ère numérique. Un système axé sur les plaintes ne permet pas d'avoir un tableau complet des violations possibles de la vie privée. Il y a peu de chances que les gens déposent une plainte à propos d'un fait dont ils ignorent l'existence. À l'ère des mégadonnées et de l'Internet des objets, on peut très difficilement savoir et comprendre ce qu'il advient de nos renseignements personnels. Cependant, le Commissariat est mieux placé pour examiner ces flux de données souvent opaques et déterminer s'ils sont appropriés sous le régime de la LPRPDE.

Une stratégie de conformité proactive permettrait aussi de procéder à des audits volontaires ou non, comme ceux que réalisent depuis longtemps certains organismes de réglementation de la protection de la vie privée dans d'autres pays et des organismes de réglementations dans d'autres domaines au Canada.

Nous proposons un modèle mettant l'accent sur une application de la loi proactive, assorti de pouvoirs d'ordonnance et de sanctions administratives pécuniaires.

Cela dit, nous continuerons de mener des enquêtes à la suite de plaintes et j'utiliserai davantage mon pouvoir d'ouvrir une enquête lorsque nous observerons des enjeux précis ou des problèmes chroniques qui ne sont pas réglés adéquatement. Mais ces pouvoirs sont limités et, en l'absence d'un motif de croire qu'il y a eu infraction, le Commissariat n'est pas habilité à réaliser des audits proactifs simplement pour vérifier la conformité. Ces pouvoirs seraient très utiles, voire nécessaires, dans un domaine comme celui de la protection de la vie privée où les modèles d'affaires et les flux de données sont souvent complexes et loin d'être transparents.

En bref, nous sommes convaincus que l'effet combiné d'une application de la loi proactive et d'une obligation de faire preuve de responsabilité serait beaucoup plus susceptible d'assurer la conformité à la LPRPDE et le respect du droit à la vie privée que le modèle actuel de l'ombudsman.

Dans le même ordre d'idées, en vertu de la loi actuelle, le Commissariat ne peut rendre d'ordonnances contraignantes ni imposer des sanctions administratives pécuniaires. Nous devons nous contenter de formuler des recommandations non contraignantes que les organisations peuvent décider de suivre ou non. Cela ne correspond pas aux pouvoirs que détiennent de nombreux homologues provinciaux

qui ont le pouvoir de rendre des ordonnances, ainsi que nos homologues internationaux - comme les États-Unis et de nombreux pays européens - qui peuvent imposer des sanctions financières qui incitent davantage les organisations à s'acquitter de leurs obligations. Il est urgent que des modifications législatives donnent au Commissariat les mêmes pouvoirs afin d'assurer un respect efficace du droit à la vie privée.

Je propose ces changements, sachant que de nombreuses organisations cherchent à se conformer à la LPRPDE et déploient des efforts considérables à cette fin. Mais ce n'est pas le cas de toutes les organisations. Or, les recommandations non contraignantes et la crainte d'une mauvaise publicité ne permettent pas toujours d'amener les entreprises à se conformer à la loi. Les sanctions seraient imposées pour promouvoir la conformité et non pour punir les organisations.

Par ailleurs, l'argument de l'industrie selon lequel le fait de modifier le modèle de l'ombudsman nuirait à la compétitivité des entreprises canadiennes ne me semble pas convaincant. La Federal Trade Commission des États-Unis peut imposer de lourdes sanctions aux entreprises américaines ayant des pratiques inéquitables en matière de protection de la vie privée. Pourtant, ces entreprises semblent pouvoir prospérer dans cet environnement.

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes a commencé à étudier en profondeur la LPRPDE. C'est une bonne nouvelle. Je lui ai fait part de certaines observations en février, mais je suis impatient de témoigner à nouveau devant lui pour discuter de notre rapport sur le consentement.

Réforme de la Loi sur la protection des renseignements personnels

Au cours de la dernière année, dans le cadre de l'examen de la *Loi sur la protection des renseignements personnels* prévu par ses propres dispositions, nous avons aussi eu la possibilité de présenter au Comité ETHI nos recommandations concernant la réforme de cette loi.

Les 16 recommandations que nous avons formulées portent sur les changements technologiques, la modernisation des normes juridiques et l'accroissement de la transparence.

Pour obtenir de plus amples renseignements concernant la réforme de la *Loi sur la protection des renseignements personnels*, consultez la page 61 du présent rapport.

À ma grande satisfaction, le Comité a affirmé dans un rapport publié en décembre qu'il est d'accord avec toutes nos recommandations. Naturellement, les représentants du gouvernement ont leurs propres objectifs en ce qui a trait à la réforme, mais ils ont aussi réagi favorablement à notre appel à la modernisation et reconnu qu'un examen global de la *Loi sur la protection des renseignements personnels* s'impose.

J'ai été particulièrement ravi lorsque des ministres se sont engagés à prendre en compte l'une de nos principales recommandations—exiger explicitement dans la loi que les organisations recueillent uniquement les renseignements *nécessaires* à un programme ou à une activité—et, en attendant la réforme législative, à réitérer aux institutions fédérales l'importance de respecter le critère de nécessité conformément à la politique du Conseil du Trésor.

Au cours de l'année qui vient, je travaillerai en collaboration avec le gouvernement afin que nous puissions ensemble donner une nouvelle vie à la *Loi sur la protection des renseignements personnels,* qui n'a

fait l'objet d'aucune mise à jour appréciable depuis son entrée en vigueur en 1983.

Cela dit, nos activités d'enquête sous le régime de la *Loi sur la protection des renseignements personnels* nous ont tenus extrêmement occupés au cours de la dernière année et nous avons le plaisir de faire connaître nos conclusions dans plusieurs dossiers importants. Par exemple, notre rapport de conclusions portant sur une série d'atteintes à la vie privée mettant en cause le système de paye Phénix du gouvernement du Canada est présenté à la page 83. Par ailleurs, nos conclusions issues d'une enquête portant sur le site Web MaDemocratie.ca du Bureau du Conseil privé visant à faire participer les Canadiens à la réforme électorale sont présentées à la page 80. Le rapport fait également état d'une enquête liée à l'utilisation des simulateurs de sites cellulaires (aussi appelés « dispositifs Stingray » ou « capteurs IMSI »), à la page 75.

Sécurité publique, sécurité nationale et surveillance exercée par le gouvernement

Outre l'avenir du consentement et la réforme législative, des questions touchant la sécurité nationale, la sécurité publique et la surveillance exercée par le gouvernement ont occupé une part importante de notre temps au cours de la dernière année.

En décembre, nous avons participé à la consultation du gouvernement concernant le *Livre vert sur la sécurité nationale*. Notre mémoire, que nous avons préparé conjointement avec les commissariats des provinces et des territoires, souligne l'importance de prendre en compte l'incidence des mesures de surveillance sur les droits et soulève des questions comme l'accès licite ainsi que la collecte et l'utilisation des métadonnées par les organismes d'application de la loi et de sécurité nationale, le chiffrement, le partage d'information par le gouvernement ainsi que la surveillance.

De façon générale, nous convenons que les enquêteurs des organismes d'application de la loi et de sécurité nationale doivent pouvoir travailler aussi efficacement dans le monde numérique que dans le monde physique. Toutefois, cela ne signifie nullement qu'il faille pour autant abaisser les seuils prévus par la loi et réduire les mesures de protection.

Au contraire, il faut maintenir les mesures de protection qui font partie de nos traditions juridiques depuis longtemps, mais en les adaptant aux réalités des outils de communication modernes, qui renferment et transmettent des renseignements personnels extrêmement sensibles. Nous avons constaté avec satisfaction que des Canadiens avaient formulé dans leur réponse au Livre vert du gouvernement des commentaires faisant écho aux nôtres.

En juin, le gouvernement a déposé le projet de loi C-59, qui porte sur la sécurité nationale. Nous comptons exprimer en temps et lieu notre point de vue sur ce projet de loi.

Plusieurs préoccupations au sud de la frontière soulèvent aussi des questions difficiles.

Des Canadiens ont dit avoir subi des interrogatoires très personnels à la frontière américaine et avoir été obligés de communiquer les mots de passe de leur ordinateur portable et de leur téléphone mobile. Nous avons mis en garde les voyageurs en leur recommandant de limiter les objets qu'ils apportent ou de supprimer les

De façon générale, nous convenons que les enquêteurs des organismes d'application de la loi et de sécurité nationale doivent pouvoir travailler aussi efficacement dans le monde numérique que dans le monde physique. Toutefois, cela ne signifie nullement qu'il faille pour autant abaisser les seuils prévus par la loi et réduire les mesures de protection.

renseignements sensibles stockés sur des appareils susceptibles d'être fouillés.

Lorsque le président américain Donald Trump a émis un décret présidentiel privant les personnes qui ne sont pas des citoyens américains ni des résidents permanents des mesures de protection prévues par la *Privacy Act* des États-Unis à l'égard des renseignements qui permettent d'identifier une personne, nous avons reçu plusieurs demandes nous priant d'examiner les répercussions pour le Canada.

Nous avons conclu que la vie privée des Canadiens bénéficie d'une certaine protection aux États-Unis. Toutefois, cette protection est précaire du fait qu'elle repose principalement sur des ententes administratives qui n'ont pas force de loi.

Nous avons exhorté les représentants du gouvernement du Canada à demander à leurs homologues américains de renforcer les mesures de protection de la vie privée des Canadiens— notamment à demander que le Canada soit ajouté à la liste des pays désignés en vertu de la *Judicial Redress Act.* Les Canadiens pourraient ainsi bénéficier de certains recours judiciaires prévus par la *Privacy Act* des États-Unis.

Nous avons aussi demandé au gouvernement de confirmer si les ententes administratives précédemment conclues entre le Canada et les États-Unis continueraient de protéger les renseignements personnels des Canadiens sur le territoire américain. Lorsque nous aurons reçu sa réponse à ce sujet, nous donnerons une orientation supplémentaire aux Canadiens afin qu'ils soient bien au fait de leurs droits et des mesures à prendre pour protéger leurs renseignements personnels quand ils se rendent à l'étranger.

On trouvera à la page 63 du présent rapport une analyse plus détaillée de notre travail effectué dans le domaine de la sécurité nationale, de la sécurité du public, des frontières et de la protection de la vie privée. Nous poursuivrons nos efforts sur ce front au cours des mois à venir.

Mot de la fin

La protection de la vie privée ne doit pas constituer une entrave à l'innovation, à l'efficacité du gouvernement ou à la sécurité nationale. Toutefois, la poursuite de ces objectifs n'est pas une raison de maintenir telles quelles des lois déficientes sur la protection des renseignements personnels ou, plus généralement, de s'en tenir aux anciennes façons de faire les choses.

C'est pour cette raison que nous voulons passer à une approche axée sur une application proactive de la loi et que nous proposons des solutions concrètes à la question du consentement. À l'aide de ressources et d'un financement adéquats, nous pourrions mettre en œuvre ces solutions dans le cadre de nos pouvoirs actuels.

Nous avons toutefois atteint un point où cela ne suffit pas. Pour que le Canada demeure un chef de file mondial de la protection de la vie privée, nous devons avoir des lois qui reflètent les réalités du XXIe siècle.

En juin, le gouvernement a déposé le projet de loi C-58, qui vise notamment à modifier la *Loi sur l'accès à l'information,* et le projet de loi C-59, qui vise à modifier le régime de surveillance des activités en matière de sécurité nationale. Ces deux domaines ont une incidence directe sur la protection de la vie privée et je suis impatient de faire part aux parlementaires de notre point de vue sur ces questions importantes.

Le gouvernement doit maintenant s'efforcer de combler les lacunes dans le régime canadien de protection de la vie privée. Des comités parlementaires et des ministres se sont montrés intéressés à explorer une réforme de la *Loi sur la protection des*

renseignements personnels et de la LPRPDE. C'est un signe encourageant.

Il ne suffit pas que le gouvernement affirme l'importance de la protection de la vie privée; il faut prendre des mesures systémiques pour la protéger.

Une très grande majorité de Canadiens se préoccupent des atteintes à leur droit à la vie privée découlant de la révolution numérique. Ils ne se sentent pas protégés par des lois qui n'ont aucun mordant ni par les organisations qui peuvent choisir de suivre ou non les recommandations non contraignantes.

Les Canadiens s'attendent à tirer parti des avantages de l'innovation, mais ils s'attendent aussi à ce que leur vie privée soit respectée.

Le moment est venu de donner aux Canadiens l'assurance que les nouvelles technologies seront mises en œuvre dans leur intérêt et qu'elles ne porteront pas atteinte à leurs droits. Les lois canadiennes sur la protection des renseignements personnels sont extrêmement désuètes, il est grand temps de les moderniser.

La protection de la vie privée en chiffres

325	Plaintes en vertu de la LPRPDE acceptées*
205	Plaintes en vertu de la LPRPDE fermées par règlement rapide*
89	Plaintes en vertu de la LPRPDE fermées à l'issue d'une enquête ordinaire*
95	Déclarations d'atteinte à la sécurité des données en vertu de la LPRPDE
1 357	Plaintes en vertu de la *Loi sur la protection des renseignements personnels* acceptées*
423	Plaintes en vertu de la *Loi sur la protection des renseignements personnels* fermées par règlement rapide*
660	Plaintes en vertu de la *Loi sur la protection des renseignements personnels* fermées à l'issue d'une enquête ordinaire*
147	Déclarations d'atteinte à la sécurité des données en vertu de la *Loi sur la protection des renseignements personnels*
95	Évaluations des facteurs relatifs à la vie privée (EFVP) reçues
49	Avis formulés à des organisations du secteur public à la suite de l'examen d'une EFVP ou d'une consultation à cet égard
3	Examens menés à bien dans le secteur public
376	Communications de renseignements dans l'intérêt public par les institutions fédérales
27	Lois et projets de loi examinés sous l'angle de leurs répercussions sur la vie privée
13	Comparutions devant des comités parlementaires sur des questions touchant les secteurs privé et public
16	Mémoires officiels présentés au Parlement sur des questions touchant les secteurs privé et public
4	Autres interactions avec des parlementaires ou leur personnel (par exemple, correspondance avec le bureau de députés ou de sénateurs)
9 091	Demandes d'information
123	Allocutions et présentations
2 012 900	Consultations du site Web
245 583	Consultations du blogue
417	Gazouillis envoyés
12 709	Abonnés sur Twitter au 31 mars 2017
57 428	Publications diffusées
50	Annonces et communiqués diffusés

* Comprend une plainte représentative pour chaque série de plaintes connexes. Pour en savoir plus, consultez l'annexe 2, « Tableaux statistiques ».

Loi sur la protection des renseignements personnels et les documents électroniques
Rétrospective de l'exercice

RAPPORT SUR LE CONSENTEMENT

Reconnu comme la pierre angulaire de la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, le consentement est l'outil qui permet aux individus d'affirmer leur autonomie et d'exercer un contrôle sur leurs renseignements personnels. La loi oblige les organisations qui souhaitent recueillir, utiliser ou communiquer des renseignements personnels à solliciter et à obtenir le consentement des intéressés. Toutefois, les avancées technologiques comme les mégadonnées, l'Internet des objets, l'intelligence artificielle et la robotique posent de sérieux défis pour les parties impliquées dans une transaction. Les organisations soutiennent qu'elles ne sont pas toujours en mesure de déterminer ou prévoir toutes les raisons pour lesquelles les renseignements personnels pourraient être utilisés ou communiqués dans le marché d'aujourd'hui en constante évolution et axé sur les données. Dans ce contexte, les efforts déployés pour expliquer les pratiques de protection de la vie privée prennent généralement la forme de politiques ou ententes sur les conditions d'utilisation formulées dans un jargon juridique, souvent incompréhensibles, qui ne cessent de changer. Il serait injuste de s'attendre à ce que les individus soient en mesure d'exercer un véritable contrôle sur leurs renseignements personnels ou de toujours prendre des décisions éclairées lorsqu'il s'agit de donner leur consentement. Voilà en quoi consiste le dilemme, qui ne peut que devenir plus complexe. Le moment est venu d'agir.

En mai 2016, le Commissariat à la protection de la vie privée du Canada a publié un document de discussion sur le consentement sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Le document visait à déterminer les améliorations à apporter au modèle de consentement actuel et définir plus clairement le rôle et les responsabilités des divers acteurs susceptibles de les mettre en œuvre. Nous avons reçu 51 mémoires en réponse au document, dont environ la moitié provenait d'entreprises ou d'associations les représentant. Les autres mémoires ont été présentés par des membres de la société civile, le milieu universitaire, le milieu juridique, les organismes de réglementation et par des citoyens. Nous avons organisé cinq tables rondes partout au pays afin d'avoir des discussions approfondies sur les défis que pose le consentement et les mesures à prendre pour les relever. Nous avons aussi

demandé le point de vue des Canadiens dans le cadre de discussions de groupe tenues dans quatre villes canadiennes. Nous souhaitons remercier tous ceux qui ont pris part à cet effort en consacrant leur temps et en apportant leur précieuse contribution.

Dans le présent chapitre, nous exposons les propos que nous avons entendus au cours de la consultation et formulons nos recommandations en vue d'améliorer le consentement afin que la LPRPDE puisse protéger efficacement la population canadienne au 21e siècle. Le document de discussion publié en mai 2016 fournit un contexte utile pour situer les concepts analysés ci-après.

Ce que nous avons entendu

Selon de nombreux intervenants, l'environnement numérique de plus en plus complexe pose des défis pour la protection de la vie privée et le modèle de consentement. Ils reconnaissent que le consentement ne convient pas toujours dans certaines situations. Par exemple, lorsque les consommateurs n'entretiennent aucune relation avec l'organisation qui utilise leurs renseignements personnels ou que les utilisations prévues des données ne sont pas connues au moment de la collecte, ou encore qu'elles sont trop complexes pour qu'on les explique aux individus. Nous avons entendu des points de vue très variés sur les mesures à prendre pour relever ces défis, mais la plupart des participants ont l'impression que le consentement devrait continuer à jouer un rôle important dans la protection de la vie privée.

Les participants aux groupes de discussion nous ont dit qu'ils pensent à la protection de leur vie privée et de leurs renseignements personnels, du moins dans une certaine mesure. En ce qui a trait à l'utilisation acceptable de leurs renseignements personnels par des entreprises, la vente ou la cession de ces renseignements à des tierces parties ne constituent pas à leurs yeux une pratique acceptable.

Les entreprises ont beaucoup insisté sur l'approche souple et neutre sur le plan technologique de la LPRPDE. Selon elles, le cadre législatif actuel est adéquat et il y a des moyens de s'attaquer aux défis sur le plan du consentement en grande partie sans modifier la loi. Toutefois, les groupes de défense des intérêts, y compris certains universitaires, avaient davantage tendance à remettre en question le statu quo. Ils recommandaient un plus large éventail de solutions pour remédier aux lacunes perçues de la LPRPDE et du modèle de consentement, par exemple le renforcement des pouvoirs d'application de la loi en général.

Les participants aux groupes de discussion sont consternés car ils ont le sentiment de ne pas avoir le contrôle sur la façon dont les entreprises recueillent et utilisent leurs renseignements personnels. Ils estiment ne pas avoir d'autre choix que de consentir à des pratiques dont ils savent peu de choses. Ils se sentent incapables de se renseigner eux-mêmes, car l'information fournie par les organisations leur semble vague, complexe et presque incompréhensible. Ils sont particulièrement préoccupés par la communication de renseignements à des tiers et s'attendent à ce qu'on leur fournisse de l'information très claire sur cette question avant de donner leur consentement. Ils veulent être mieux renseignés afin de pouvoir exercer un contrôle individuel, mais s'attendent aussi à ce que le gouvernement leur offre une meilleure protection, car c'est lui qui possède le plus de connaissances et les meilleurs outils pour assurer le respect de la vie privée.

On trouvera ci-après des suggestions et des commentaires formulés par les intervenants, suivis par la réponse du Commissariat, qui propose des mesures à prendre et formule des recommandations.

Modèle amélioré de consentement

De nombreux participants ont exprimé leur point de vue sur l'importance du consentement et le rôle que les solutions de remplacement pourraient jouer dans l'avenir. Les intervenants qui croient le plus fermement au consentement considèrent la protection de la vie privée comme la protection du droit des individus de décider par eux-mêmes de ce qu'il advient de leurs renseignements personnels, et le consentement, comme le moyen d'exercer leur autonomie. Certains estiment que les difficultés liées au consentement découlent non pas de la notion de consentement en soi, mais de la façon dont elle est mise en pratique. Certains ont aussi affirmé que le consentement devrait être un processus continu plutôt qu'un choix fait une seule fois qui ne laisserait pas de place à une solution intermédiaire. À signaler toutefois que dans certaines situations, le consentement risque d'imposer une trop grande responsabilité aux individus, comme dans le cas du traitement algorithmique des mégadonnées, trop complexe pour le citoyen ordinaire, et où les futures utilisations des renseignements ne sont pas toujours connues immédiatement.

Forme de consentement

Nous avons entendu beaucoup de discussions sur la forme que devrait prendre le consentement. Des participants ont suggéré au Commissariat de préciser les situations où un consentement explicite est requis et celles où un consentement implicite pourrait être acceptable. Certains ont proposé d'exiger un consentement positif lorsque les fins de l'utilisation des renseignements ne sont pas d'emblée évidents. Par contre, d'autres ont indiqué que le consentement à la collecte de renseignements personnels qui sont vraiment nécessaires pour obtenir un bien ou un service pourrait être implicite, à quelques exceptions près. D'autres encore ont mentionné que les types d'avis ou de choix prévus devraient être fonction de la sensibilité des renseignements ou du risque de préjudice découlant d'une activité de traitement de données. Selon certaines personnes, le Commissariat devrait élargir la portée du consentement implicite tout en imposant une plus grande responsabilité aux organisations quant au traitement des renseignements personnels.

Politiques de confidentialité simplifiées

Les auteurs de quelques mémoires ont recommandé d'utiliser des politiques de confidentialité courtes ou simplifiées, mais nous avons constaté dans l'ensemble peu d'intérêt pour les politiques ou les modèles génériques. De l'avis général, pour être utiles, les pratiques de protection de la vie privée doivent être énoncées dans le contexte particulier du service offert. Même dans un secteur industriel donné, il serait difficile de définir des pratiques de protection de la vie privée génériques. Selon certains participants, les organisations devraient veiller à indiquer clairement, dès le début, les renseignements essentiels que les individus rechercheront lorsqu'on sollicitera leur consentement. Par exemple, quels seraient les renseignements recueillis, quelle utilisation en serait faite, à qui ils seraient communiqués et à quelles fins. Il faudrait accorder une attention particulière aux risques imprévus ou aux pratiques potentiellement préjudiciables. Certains ont suggéré que le Commissariat précise les pratiques exemplaires en donnant des orientations ou en publiant des codes de pratique.

De nombreux participants ont recommandé d'adopter des politiques de confidentialité plus courtes, ou à plusieurs niveaux. Une suggestion est revenue souvent : permettre aux organisations de signaler uniquement les pratiques qui s'écartent de la norme, en éliminant les exigences réglementaires normalisées communes à l'échelle de l'industrie ou les longues explications de pratiques qui seraient ou devraient être évidentes pour les utilisateurs compte tenu du service. D'autres privilégient les avis de consentement en temps réel ainsi que l'utilisation d'infographie, de vidéos et d'agents virtuels pour compléter l'information figurant dans les politiques de confidentialité. D'autres encore ont réclamé davantage de recherches sur des mécanismes novateurs pour transmettre de l'information sur la protection de la vie privée.

Certains intervenants ont critiqué les politiques de confidentialité en général en les comparant aux contrats d'adhésion du fait qu'elles sont « à prendre ou à laisser ». On nous a dit qu'il est important d'obtenir le consentement au bon moment au cours du processus afin qu'il soit valable. Des participants aux groupes de discussion déplorent généralement le fait que l'acceptation des conditions d'utilisation soit le prix à payer pour faire affaire avec des entreprises. Selon eux, le consentement est rarement éclairé, voire jamais. C'est une transaction ne laissant pas de place à une solution intérimaire, sur laquelle ils n'ont aucun contrôle.

Solutions technologiques

Les solutions technologiques visant à améliorer le consentement sont généralement bien perçues, mais selon certains, elles sont encore relativement nouvelles dans un environnement numérique en évolution rapide.

Parmi les solutions présentées dans les mémoires figure l'« étiquetage » des données afin d'en limiter la collecte, l'utilisation, la communication et la conservation. Certains mémoires font aussi référence au concept d'« accusés de réception du consentement » pour exercer un contrôle sur les choix futurs. D'autres encore recommandent d'utiliser un tableau de bord ou un portail pour surveiller et ajuster les paramètres de confidentialité. Par ailleurs, les auteurs d'un mémoire ont suggéré d'adopter des mesures techniques pour masquer ou dissimuler certains éléments d'information et protéger ainsi uniquement les données qui doivent être protégées tout en permettant d'utiliser en toute liberté les autres éléments d'information.

D'après certains, la technologie pourrait aider à gérer la complexité et on pourrait adopter des paramètres pour déterminer si les pratiques de gestion des données de l'entreprise respectent les préférences des individus en matière de consentement. Il a été suggéré que le Commissariat indique les meilleures solutions existantes parmi les différentes approches, par exemple les outils de déclaration liés à la protection de la vie privée, les tableaux de bord sur les choix, l'infrastructure, la structure des bases de données et les outils de transparence. Des participants ont aussi affirmé que le Commissariat devrait encourager fortement les géants des technologies à intégrer dans leurs systèmes d'exploitation des solutions qui facilitent le consentement.

Désidentification

Selon de nombreux participants, la désidentification semble présenter des avantages pour la protection de la vie privée, mais elle comporte des risques importants. D'une part, on peut y recourir pour trouver un équilibre entre la protection des renseignements personnels et le souhait des organisations d'utiliser ces renseignements de façons nouvelles et novatrices. D'autre part, on s'inquiète du fait qu'il puisse tout simplement être impossible de désidentifier complètement les renseignements personnels sans qu'il reste un risque de réidentification.

Plusieurs participants de l'industrie et du milieu juridique ont fait valoir que les renseignements désidentifiés ne sont pas des renseignements personnels, qu'ils ne relèvent pas de la LPRPDE et qu'il n'est donc pas nécessaire d'obtenir le consentement des intéressés pour les recueillir, les utiliser ou les communiquer. D'autres, notamment des représentants du milieu universitaire et de la société civile, sont d'avis que la LPRPDE devrait continuer de s'appliquer même à ces renseignements, compte tenu du risque réel et croissant de réidentification et de la nécessité de s'assurer que les organisations continuent de rendre compte de leur utilisation des renseignements désidentifiés, y compris l'utilisation à des fins responsables et les mesures de protection appropriées. Certains participants considèrent la désidentification et les filets de sécurité contractuels contre la réidentification comme des stratégies utiles pour réduire le plus possible les risques de collecte, d'utilisation et de communication non autorisées des renseignements personnels, mais pas nécessairement comme une solution de remplacement du consentement.

Des représentants de l'industrie ont demandé au Commissariat des orientations sur des questions comme les méthodes de désidentification et l'évaluation du risque de réidentification, afin de compléter les orientations émanant d'autres autorités de protection des données. Ainsi, les organisations réduiraient le risque de réidentification et parviendraient à un meilleur équilibre entre la protection de la vie privée et les fins commerciales.

Protection de la vie privée dès la conception et protection de la vie privée par défaut

En général, les intervenants se sont dits favorables au principe de protection de la vie privée dès la conception d'un produit ou d'un service et estiment qu'il devrait être encouragé. Cependant, ils ont fait une mise en garde contre l'adoption d'une approche trop normative, car elle risquerait de nuire à l'innovation et à la compétitivité. Selon l'industrie, bien qu'il s'agisse d'un bon principe directeur, la protection de la vie privée dès la conception ne doit pas être prévue dans la loi puisqu'elle est déjà reconnue comme pratique exemplaire.

En revanche, l'acceptation de la protection de la vie privée par défaut ne fait pas l'unanimité. Certains participants estiment qu'elle optimiserait le contrôle exercé par l'utilisateur, tandis que d'autres sont d'avis qu'elle est trop compliquée et qu'elle entraverait l'utilisation pratique et continue d'un produit ou d'un service. Nombreux sont ceux qui estiment que les mesures de contrôle en matière de protection de la vie privée dépendent du type de service offert et qu'elles devraient refléter les préférences personnelles des individus, qui peuvent être plus ou moins à l'aise de communiquer leurs renseignements personnels.

Zones interdites

En règle générale, les participants ne souhaitent pas que la loi définisse des zones interdites particulières. Le concept des zones interdites est fondé sur l'idée, reconnue au paragraphe 5(3) de la LPRPDE, que la collecte, l'utilisation et la communication des renseignements personnels devraient être carrément prohibée dans certains cas, peu importe si le consentement a été obtenu ou non. La plupart des participants estiment que le paragraphe 5(3) de la LPRPDE est suffisant pour gérer les situations de « zones interdites » avec souplesse, sans qu'il soit nécessaire de les prévoir expressément dans la loi. Des participants ont fait une mise en garde contre l'imposition d'une trop grande réglementation dans un environnement en évolution rapide ou contre le recours à des mesures de protection imposées d'en haut au lieu de donner le pouvoir aux individus. Ils reconnaissent toutefois que certaines pratiques, comme l'écoute non autorisée au moyen d'appareils connectés, sont particulièrement contestables et inappropriées.

Certains groupes de la société civile sont en faveur des zones interdites et suggèrent même des exemples d'utilisations prohibées à envisager, notamment : i) l'enregistrement sonore par le microphone ou la caméra d'un utilisateur, sauf dans les cas où ce dernier se sert de ces fonctions pour obtenir des services sur le site; ii) la publication de renseignements personnels afin d'inciter les personnes à payer un montant pour faire retirer leurs renseignements; iii) la tentative de réidentifier un utilisateur à partir de données anonymisées.

Intérêts légitimes

Peu de participants souhaitent que les intérêts légitimes deviennent un nouveau motif pour le traitement des données, mais on reconnaît que la délimitation du consentement est étirée au-delà des limites dans certaines situations. Par exemple, certains ont fait remarquer que les intermédiaires comme les moteurs de recherche ne peuvent pas demander le consentement comme condition pour fournir des milliards de résultats de recherches effectuées quotidiennement et susceptibles de contenir ou non des renseignements personnels. De plus, dans le contexte des mégadonnées, il y a constamment de nouvelles possibilités d'analyser d'énormes quantités de données obtenues initialement à une fin et combinées avec diverses autres sources de données afin de trouver de nouvelles possibilités novatrices. Ces possibilités ne peuvent cependant pas toujours

être prévues au moment de la collecte initiale, de la même façon qu'il est pratiquement impossible de recommuniquer avec chaque personne afin d'obtenir à nouveau son consentement, comme l'exige la LPRPDE.

De nombreux universitaires et groupes de la société civile craignent qu'une approche axée sur les intérêts légitimes ne réduise considérablement le contrôle exercé par les individus en raison de son caractère non limitatif. Ils sont sceptiques à l'idée d'intégrer dans la LPRPDE un concept européen ancré dans un contexte législatif complètement différent. À leur avis, il existe dans le contexte européen des mesures de protection complémentaires beaucoup plus efficaces que c'est actuellement le cas dans la LPRPDE.

De son côté, l'industrie n'est pas très favorable au concept non plus. Selon des participants, il serait peut-être préférable d'étendre le concept de consentement implicite, puisque l'on peut retirer son consentement, tandis que l'on ne peut mettre de côté les intérêts légitimes. Il y a aussi des arguments en faveur d'une description générale des fins visées (comme « améliorer le service à la clientèle ») qui autoriserait les organisations à utiliser les renseignements à des fins non connues au moment de la collecte. D'autres croient que le moment est venu de reconnaître les limites du consentement et qu'il faudrait peut-être un nouveau concept pour trouver un équilibre entre les besoins de l'industrie et la protection de la vie privée.

Sans s'opposer au concept des intérêts légitimes, certains participants craignent que le profit puisse l'emporter sur les intérêts individuels et publics si les organisations seules définissent ce concept. Une solution possible consisterait à demander que la justification de la décision reposant sur les intérêts légitimes soit communiquée à l'organisme de réglementation ou soumise à l'examen d'un tiers.

Éthique

Quelques mémoires appuient les évaluations et les cadres éthiques, y compris la création de comités d'éthique indépendants composés de tiers. Toutefois, les participants aux réunions des intervenants—qu'ils soient issus de l'industrie, de la société civile ou d'autres organismes de réglementation—étaient généralement plutôt sceptiques à cet égard.

Aux yeux de certains participants, cette approche risque d'être paternaliste du fait qu'elle permettrait aux membres des comités d'éthique de parler au nom d'individus. D'autres sont préoccupés par la faisabilité opérationnelle des comités d'éthique, soit parce que ces comités entraîneraient un coût trop élevé pour les petites entreprises, soit parce qu'ils créeraient un fardeau administratif inutile. De grandes entreprises ont déjà commencé à mettre en place des comités consultatifs internes en matière d'éthique, mais certaines d'entre elles doutent que les organisations acceptent de communiquer des renseignements commerciaux confidentiels à des tiers de l'extérieur ou d'être liées par des avis externes. D'autres participants ont indiqué qu'il existe d'autres façons de gérer les utilisations non éthiques des données, par exemple en invoquant le paragraphe 5(3) de la LPRPDE ou en renforçant l'application de la loi.

Application de la loi

Les groupes d'intervenants ont exprimé des points de vue divergents sur la nécessité de renforcer les pouvoirs d'application de la loi conférés au Commissariat. Les organisations considèrent généralement qu'il n'y a pas lieu de les renforcer. Certaines estiment que la menace de communiquer dans l'intérêt public l'identité des organisations fautives suffit à les amener à se conformer en raison de l'atteinte à leur réputation qui pourrait en découler. On a fait remarquer que des pouvoirs accrus auraient pour effet d'augmenter considérablement les coûts de la conformité et que l'application de la loi doit se faire de la façon la plus efficace possible en termes de coûts afin de ne pas entraver l'innovation. Certains

Les Canadiens ont dit qu'ils veulent un commissaire à la protection de la vie privée qui peut renforcer les mesures d'application de la loi, avec des pouvoirs de rendre des ordonnances, et la possibilité d'imposer des amendes.

participants sont d'avis que le renforcement des pouvoirs d'application n'est pas la solution parce que les organisations canadiennes veulent généralement respecter la LPRPDE; ils ont aussi fait une mise en garde contre des pouvoirs renforcés qui pourraient freiner l'innovation au sein des organisations, car celles-ci craindraient de ne pas se conformer. D'autres pensent que l'on obtiendrait une plus grande conformité en sensibilisant davantage les organisations aux exigences de la LPRPDE qu'en misant sur l'application de la loi.

De façon générale, les représentants de la société civile et du milieu universitaire demandent un renforcement des pouvoirs d'application de la loi, soutenant que l'autoréglementation ne fonctionne pas à l'heure actuelle. Certains sont d'avis que l'application de la loi est l'outil le plus efficace pour défendre le respect de la vie privée; pourtant, la loi n'est pas suffisamment appliquée. On a fait remarquer que les PDG accordent inévitablement plus d'attention aux domaines où ils risquent de faire face à des mesures d'application de la loi, c'est-à-dire ceux où des organismes de réglementation nationaux ou internationaux possèdent un plus grand pouvoir de rendre des ordonnances et peuvent imposer des amendes. Les PDG investissent davantage de ressources pour assurer leur conformité dans ces domaines.

Les consommateurs s'attendent manifestement à un renforcement des mesures d'application de la loi, quelle qu'en soit la forme : ordonnances, amendes ou vérifications. On nous a dit qu'il est peu probable qu'une plainte soit déposée dans certaines situations et que l'organisme de réglementation doit donc être plus proactif en matière de surveillance de la conformité. Certains intervenants demandent un abaissement des seuils de vérification. L'autovérification des entreprises a aussi été soulevée. Toutefois, certaines organisations s'opposent à ce qu'elles considèrent comme un renversement du fardeau de la preuve dans le cadre d'un système proactif de vérification.

Certains ont proposé que le Commissariat exprime, sur demande, une opinion préliminaire sur une pratique proposée par une entreprise. Une organisation de la société civile a recommandé que le commissaire soit habilité à délivrer aux frais des entreprises des « lettres d'accord présumé » où il exprimerait une opinion préliminaire sur la conformité d'une pratique proposée à la LPRPDE.

Éducation

La plupart des participants aux groupes de discussion souhaitent disposer de matériel éducatif sur des questions relatives à la protection de la vie privée. L'information jugée la plus utile comprend les éléments importants d'une politique de confidentialité, les données à ne pas communiquer à d'autres entreprises, les mesures prises par le gouvernement pour protéger les renseignements

Les participants aux groupes de discussion ont manifesté un désir généralisé de recevoir de l'information sur des questions relatives à la protection de la vie privée de la part du gouvernement grâce à des efforts de sensibilisation ou d'éducation publique, incluant par exemple, les éléments à prendre en considération dans les politiques de confidentialité et l'information à ne pas divulguer/partager.

personnels ainsi que les droits et les obligations des individus.

Des intervenants appuient également les efforts d'éducation du public, mais certains ont fait une mise en garde contre le recours à l'éducation pour refiler aux individus les responsabilités en matière de protection des renseignements personnels.

De nombreux intervenants ont formulé des commentaires sur l'importance de l'orientation donnée par le Commissariat et ont recommandé qu'il émette des orientations supplémentaires. Les sujets d'intérêt sont notamment la désidentification, les formes de consentement et les outils pratiques destinés aux petites et moyennes entreprises. Certains ont également appelé le Commissariat à préciser ses attentes concernant la conformité dans certains domaines, comme les véhicules intelligents.

Des participants ont affirmé que le Commissariat et les organisations sont tenus d'établir des normes acceptables pour la plupart des individus. D'autres ont suggéré de récompenser les pratiques exemplaires afin de corriger la perception que la protection des renseignements personnels entrave l'innovation et complique les choses.

Les participants ont discuté du recours aux codes de pratique pour fournir aux organisations des précisions sur leurs obligations en vertu de la loi et donner aux individus l'assurance que les organisations adhérant aux codes respectent leurs obligations en matière de protection de la vie privée. Les intervenants sont partagés concernant l'utilité des codes de pratique. Des entreprises font valoir que les codes de pratique sectoriels « universels » ne reflètent pas la diversité des pratiques et les besoins des entreprises dans l'économie numérique. Toutefois, certaines sont en faveur des codes associés aux activités élaborés avec le concours des intervenants visés.

Selon des participants, les organisations devraient être tenues de piloter les initiatives sur les codes de pratique, car ce sont elles qui connaissent le mieux leur entreprise; elles pourraient cependant avoir besoin d'encouragement en ce sens. Les bonnes entreprises peuvent se servir d'un code de pratique pour inciter les « mauvais élèves » à se conformer et les amener à améliorer leurs pratiques, ce qui pourrait aussi favoriser une culture du respect de la vie privée et ainsi améliorer la réputation des organisations et renforcer la confiance des consommateurs.

Notre point de vue

Le consentement demeure au cœur de l'autonomie personnelle, mais il faut ajouter d'autres mécanismes pour l'appuyer et ainsi protéger la vie privée plus efficacement. Notamment, des organismes de réglementation indépendants qui renseignent les citoyens, orientent l'industrie, lui demandent des comptes et sanctionnent les comportements inacceptables. On doit aussi envisager d'autres outils de protection de la vie privée dans des situations exceptionnelles et justifiables où cela est pratiquement impossible d'obtenir le consentement.

Le consentement est un élément fondamental de la LPRPDE. En vertu de cette loi, une organisation doit obtenir le consentement valable d'un individu pour recueillir, utiliser et communiquer ses renseignements personnels, sauf dans certains cas d'exception. Au moment de l'adoption de la LPRPDE, les interactions avec les entreprises étaient généralement prévisibles, transparentes et bilatérales. Les consommateurs comprenaient bien pourquoi l'entreprise avec laquelle ils faisaient affaire avait besoin de certains renseignements personnels.

Le consentement demeure au cœur de l'autonomie personnelle, mais il faut ajouter d'autres mécanismes pour protéger la vie privée plus efficacement. Notamment, des organismes de réglementation indépendants qui renseignent les citoyens, orientent l'industrie, lui demandent des comptes et sanctionnent les comportements inacceptables.

Il y avait des moments bien définis où les entreprises recueillaient des renseignements et obtenaient le consentement. Mais il est devenu de plus en plus difficile d'obtenir un consentement valable dans l'environnement numérique.

Dans le document de discussion sur le consentement, nous décrivons les nombreux défis que posent les nouvelles technologies et les nouveaux modèles d'affaires pour le modèle de consentement prévu dans la LPRPDE. Le recours à des politiques de confidentialité obscures comme fondement au consentement, les flux d'information complexes et les processus opérationnels faisant intervenir une multitude de tiers intermédiaires, notamment les moteurs de recherche, les plateformes et les agences de publicité, exercent des pressions sur le modèle de consentement. À l'ère des mégadonnées, de l'Internet des objets, de l'intelligence artificielle et de la robotique, les consommateurs ne savent plus très bien qui traite les données les concernant et à quelles fins. Pour les individus, le prix à payer pour utiliser des services numériques modernes consiste à accepter, dans une certaine mesure, que leurs renseignements personnels soient inévitablement recueillis et utilisés par les entreprises pour bénéficier d'un produit ou d'un service.

C'est pourquoi l'applicabilité du modèle de consentement actuel a été remise en question. Nous tenons toutefois à préciser qu'à notre avis, le consentement continue de jouer un rôle important dans la protection du droit à la vie privée, dans les situations où la personne concernée dispose d'information suffisante pour donner un consentement valable. Les intervenants et les groupes de discussion ont suggéré toute une gamme de mesures pour améliorer le consentement.

Les situations où cela est pratiquement impossible d'obtenir le consentement sont probablement très précises—par exemple lorsqu'il n'existe aucune relation entre un individu et l'organisation qui recueille et utilise les renseignements personnels, comme les moteurs de recherche. Il peut être pratiquement impossible (ou du moins très difficile) d'obtenir un consentement valable dans le cas d'initiatives de mégadonnées ou d'appareils de l'Internet des objets que les gens n'ont d'autre choix que d'utiliser. Il se pourrait que certains modes de fonctionnement de la technologie empêchent de comprendre comment les renseignements personnels sont traités ou quelles peuvent être les conséquences, ce qui affaiblit la pertinence et la validité du consentement éclairé.

Lorsqu'il est pratiquement impossible d'obtenir le consentement, la difficulté consiste à déterminer ce que l'on peut faire pour maintenir des mesures efficaces de protection des renseignements personnels dans un contexte où la technologie, les entreprises et la société exercent des pressions qui évoluent constamment ainsi qu'à préciser les améliorations à apporter au mode de consentement actuel.

Les progrès technologiques procurent des avantages considérables aux individus. Ils facilitent grandement les communications et donnent accès à une mine de renseignements ainsi qu'à des produits et services venant de toutes les régions du monde. Toutefois, les technologies créent aussi des risques d'atteinte à la vie privée. Des mesures efficaces de protection de la vie privée sont essentielles pour maintenir la confiance des consommateurs et favoriser une économie numérique vigoureuse et novatrice à laquelle les individus ont le sentiment de pouvoir participer avec assurance. Les nouvelles technologies sont aussi porteuses d'avantages considérables pour la société, et la croissance économique future reposera en grande partie sur l'économie numérique. Par exemple, le Canada est bien placé pour devenir un chef de file mondial de l'intelligence artificielle, qui dépend de la collecte et de l'utilisation d'énormes quantités de données. Le gouvernement fédéral a déjà beaucoup investi dans le domaine en raison de l'excellent potentiel de rendement. Par ailleurs, le Canada est

un signataire de la Déclaration ministérielle de l'OCDE sur l'économie numérique publiée en 2016 et s'est engagé notamment à déployer des efforts à l'échelle internationale pour protéger la vie privée, reconnaissant son importance pour la prospérité économique et sociale.

Pourtant, selon le Sondage auprès des Canadiens sur la protection de la vie privée mené par le Commissariat en 2016, la grande majorité des Canadiens craignent de perdre le contrôle qu'ils exercent sur leurs renseignements personnels—92 % ont exprimé une certaine préoccupation au sujet de la protection de leur vie privée. De ce nombre, 57 % étaient énormément préoccupés par cette question. Si l'on n'améliore pas considérablement la protection de leur vie privée, les Canadiens perdront confiance dans l'économie numérique, ce qui entravera sa croissance et limitera leur capacité de bénéficier de tous les avantages découlant de l'innovation. L'un des objectifs stratégiques du Commissariat consiste à renforcer la protection de la vie privée et la confiance des individus pour qu'ils puissent participer avec assurance à l'économie numérique innovante. C'est pourquoi nous mettons l'accent sur le consentement.

Une très grande majorité de Canadiens sont préoccupés. Ils ont des craintes réelles. Il est temps de leur donner l'assurance que les nouvelles technologies les serviront et ne constitueront pas une menace à leurs droits.

L'absence de solides mesures de protection de la vie privée aura probablement aussi des conséquences pour la société. Les internautes veulent exprimer leur opinion, explorer celle des autres et faire des recherches sur des questions sensibles comme la santé, sans craindre que ces activités les mettent dans l'embarras et qu'elles soient utilisées contre eux ou communiquées à des tiers ayant des intérêts opposés aux leurs. La confidentialité et le consentement éclairé aident à soutenir notre régime démocratique où les individus peuvent exercer leur droit à l'autonomie, dont celui de faire des choix et d'exprimer des préférences. Nous devons examiner de façon critique toute situation qui risque de porter atteinte à notre autonomie et travailler à créer un environnement où les individus pourront se servir d'Internet pour explorer leurs intérêts et se développer comme personnes sans craindre que leur trace numérique n'entraîne un traitement injuste[1].

Dans le cadre de nos efforts en vue de trouver des solutions qui permettraient de renforcer les mécanismes de protection de la vie privée aujourd'hui et dans l'avenir, nous avons fait face au dilemme fondamental du mode de partage de la responsabilité de la protection de la vie privée entre les différents acteurs—les individus, les organisations, les organismes de réglementation et les législateurs. Un intervenant a fait valoir le point de vue convaincant que les individus doivent demeurer au centre de la protection de la vie privée, mais qu'ils ont besoin de tiers fiables comme des organismes de réglementation pour jouer un rôle plus proactif en protégeant davantage leurs intérêts.

En fait, dans l'écosystème numérique actuel, il n'est plus juste de demander aux consommateurs d'assumer toute la responsabilité d'avoir à décortiquer des flux complexes de données afin de pouvoir faire un choix éclairé pour ce qui est de donner ou non leur consentement. L'autonomie est très importante. Toutefois, compte tenu de la complexité de l'environnement, les organismes de réglementation possédant l'expertise voulue pour renforcer la protection de la vie privée au moyen de l'éducation et de l'application proactive des lois ont un rôle important à jouer. Les organisations aussi doivent faire preuve de transparence à l'égard de leurs pratiques et respecter le droit des individus à faire des choix en matière de confidentialité. De plus, les législateurs doivent intervenir lorsque les lois ne permettent plus d'atteindre l'objectif fixé au départ ni de protéger les Canadiens du risque de préjudice.

1 Il s'agit aussi d'un des objectifs liés aux priorités stratégiques du Commissariat.

En d'autres termes, tout le monde—les individus, les organisations, les organismes de réglementation et les législateurs—doit apporter sa contribution pour que la vie privée soit bien protégée. Comme il était indiqué dans le document de discussion sur le consentement, le fardeau de comprendre des pratiques compliquées et d'y consentir ne devrait pas reposer uniquement sur les épaules des individus. Il faut mettre en place des mécanismes de soutien appropriés pour faciliter le processus de consentement. Par conséquent, nous proposons que tous les acteurs concernés examinent les solutions qui suivent.

Renforcement de la validité du consentement

Avis de confidentialité

Pour s'attaquer aux situations où on peut difficilement obtenir le consentement, il est important de s'attarder en premier lieu aux mécanismes de consentement en place, aux améliorations qui peuvent y être apportées et à la façon de procéder. De nombreuses situations, dont celles liées aux nouvelles technologies et aux nouveaux modèles d'affaires, continueront de nécessiter le consentement des individus. Pour que le consentement soit valide, les individus doivent comprendre la nature, la fin et les conséquences de la collecte, de l'utilisation et de la communication de leurs renseignements personnels. Même si la LPRPDE ne mentionne pas explicitement les politiques de confidentialité, la plupart des entreprises ont choisi cette politique ou les conditions d'utilisation comme principal véhicule pour obtenir un consentement éclairé et satisfaire aux diverses autres exigences législatives et réglementaires. C'était un choix discutable dès le départ et ces documents ont continué au fil du temps de devenir de plus en plus longs et complexes. Le problème s'est amplifié à mesure que les entreprises se lançaient en ligne en omettant généralement d'adapter leur avis de confidentialité à l'environnement numérique. Elles ont plutôt simplement converti un document analogue, ponctuel et statique en format électronique.

Au cours des consultations, les politiques de confidentialité ont été grandement critiquées, parce qu'elles brouillent les pratiques de traitement des données en étant trop longues, qu'elles utilisent une terminologie complexe et ambiguë et qu'elles ne donnent généralement pas aux individus une description claire du mode de gestion de leurs renseignements personnels. Des participants ont mentionné la complexité, le manque de clarté et l'approche du tout ou rien des mécanismes de consentement. D'après ce que nous avons entendu, les politiques de confidentialité ne fonctionnent pas dans l'esprit de l'utilisateur moyen. Bon nombre de participants aux groupes de discussion n'avaient pas d'idée claire ou définie de ce que cela signifie lorsqu'une entreprise a une politique de confidentialité et la plupart ont admis ne pas la lire.

Les participants ont discuté longuement des mesures à prendre pour améliorer les politiques de confidentialité. Ils ont proposé diverses mesures, entre autres la mise en évidence des utilisations imprévues des renseignements personnels et l'élaboration de politiques multimédias et interactives. Nous convenons que les politiques de confidentialité ont été inefficaces dans la perspective du consentement, mais elles servent néanmoins diverses fins juridiques importantes. Elles sont le fondement du modèle contractuel de l'avis et du consentement en vigueur. En outre, les organismes de réglementation et les autres intervenants doivent se reporter aux politiques de confidentialité pour tenir les organisations responsables de leurs pratiques de gestion des renseignements personnels et des autres obligations qui leur incombent en vertu de la loi.

Certains intervenants ont demandé au Commissariat d'élaborer des modèles de politiques de confidentialité propres à différents secteurs. Nous ne croyons cependant pas que cela soit le rôle d'un organisme de réglementation. Il serait préférable de laisser les organisations trouver des solutions novatrices et créatives pour appuyer le processus de consentement d'une manière qui respecte la nature de leurs relations

avec les consommateurs. Toutefois, ce faisant, nous encourageons les organisations à se laisser guider par les principes suivants :

1. Toute l'information fournie sur la collecte, l'utilisation et la communication de renseignements personnels doit être facilement accessible, mais, pour éviter une surabondance d'information et faciliter la compréhension des individus, il faut mettre de l'avant certains éléments clés (voir ci-après) afin d'obtenir un consentement éclairé.

2. L'information doit être communiquée aux individus par couches gérables et facilement accessibles, et ceuxci devraient avoir la possibilité de déterminer à quel point et quand ils souhaitent obtenir des renseignements plus détaillés.

3. Les individus doivent pouvoir choisir facilement « oui » ou « non » quand il s'agit de la collecte, de l'utilisation ou de la communication de renseignements qui ne sont pas essentiels à l'achat d'un produit ou à la prestation d'un service.

4. Les organisations devraient concevoir ou adopter des processus de consentement novateurs qui peuvent être mis en œuvre juste à temps et qui sont propres au contexte et appropriés au type d'interface utilisé.

5. Les processus de consentement doivent prendre en compte la perspective du consommateur afin qu'ils soient conviviaux et que l'information fournie soit généralement compréhensible du point de vue du public cible visé par les organisations.

6. Les organisations devraient pouvoir montrer sur demande les mesures qu'elles ont prises pour vérifier si leurs processus de consentement sont vraiment conviviaux et compréhensibles du point de vue du public cible.

7. Le consentement éclairé est un processus continu qui change selon les situations; les organisations ne devraient pas s'en tenir à un moment statique dans le temps, mais elles devraient plutôt traiter le consentement comme un processus dynamique et interactif.

Comme il est indiqué dans les Lignes directrices en matière de consentement en ligne publiées conjointement en 2014, le consentement obtenu par les organisations doit reposer sur de l'information exhaustive et compréhensible et, par conséquent, cette information doit être facilement accessible. Toutefois, nous croyons qu'il faut mettre de l'avant certains éléments afin d'obtenir un consentement valable, à savoir :

- quels renseignements personnels sont recueillis;
- à qui ils sont communiqués, dont une énumération des tiers;
- à quelles fins les renseignements sont recueillis, utilisés ou communiqués, y compris une explication des fins non essentielles à la prestation du service;
- quel est le risque de préjudice pour l'individu, le cas échéant.

Les organisations devraient donner la bonne information aux individus au moment où ils en ont le plus besoin, par exemple utiliser un langage clair et ne pas décrire vaguement les fins prévues en s'en tenant à des phrases comme « améliorer l'expérience client ». Nous reconnaissons qu'il est difficile de trouver le point d'équilibre entre fournir aux utilisateurs l'information dont ils ont besoin afin de prendre des décisions éclairées et ne pas interrompre le déroulement de leur expérience ni causer de la lassitude à l'égard du consentement. Néanmoins, c'est seulement lorsque les individus disposent de la bonne information au bon moment et dans un format compréhensible qu'ils peuvent exercer un véritable contrôle sur leurs renseignements personnels.

Nous mettrons à jour nos lignes directrices en matière de consentement en ligne afin de préciser quatre éléments clés qui doivent être mis en évidence dans les avis de confidentialité et expliqués de manière conviviale.

Dans le cadre de nos activités de vérification de la conformité, nous continuerons d'obliger les organisations à fournir une information exhaustive, mais nous nous attendrons aussi à ce qu'elles accordent une importance accrue aux quatre éléments susmentionnés. Nous avons mis à jour les lignes directrices en matière de consentement en ligne afin de clarifier ces attentes et nous vous invitons à formuler des commentaires sur le changement proposé.

Formes de consentement

Des intervenants ont aussi posé des questions sur la forme de consentement qui devrait être exigée dans une situation donnée. Selon certains, le consentement devrait être explicite en ce qui concerne les pratiques proposées qui ne sont pas fondamentales ou essentielles à la prestation du service ou qui sont imprévues ou hors contexte. Par ailleurs, les individus ne veulent pas qu'on leur demande trop souvent leur consentement explicite. Encore une fois, nous reconnaissons que l'effet lassant d'avoir à donner son consentement va à l'encontre de l'intérêt de tous, aussi bien les individus que les entreprises. Les tribunaux ont affirmé que les organisations appelées à choisir la forme de consentement à utiliser doivent alors prendre en compte la sensibilité des renseignements ainsi que les attentes raisonnables de l'individu, deux aspects tributaires du contexte[2]. Nous examinerons de quelle façon nous pouvons mieux préciser le concept d'attente raisonnable des individus dans différents contextes. À cette fin, il faudra peut-être collaborer avec les organisations et les individus pour déterminer quels renseignements personnels ils considèrent comme étroitement liés à la prestation des services. Nous nous attendrons à ce que les organisations fassent preuve d'une grande transparence quant aux situations où des renseignements personnels sont fondamentaux ou essentiels à la prestation du service et de celles où ils ne le sont pas.

Nous sommes aussi d'accord avec les intervenants selon lesquels la forme de consentement devrait dépendre de la sensibilité des renseignements et du risque de préjudice découlant d'une activité de traitement des données. La LPRPDE fait mention de la sensibilité, mais il n'est pas explicitement question du risque de préjudice. Pourtant, nous considérons ce risque comme un important facteur connexe à prendre en compte au moment d'évaluer la sensibilité des renseignements personnels dans un contexte donné. Nous modifierons donc en conséquence nos lignes directrices sur le consentement et nous demanderons au Parlement de faire du risque de préjudice un facteur explicite à prendre en compte pour déterminer la forme de consentement acceptable.

Enfants et jeunes

Pendant les consultations sur le consentement, certains intervenants ont demandé une orientation concernant l'application aux enfants des exigences de la LPRPDE en la matière. Selon nous, la capacité d'un enfant à donner un consentement valable dépend de son degré de maturité. Or, la maturité est un processus de développement cognitif et social en évolution. La capacité de donner un consentement valable peut varier d'un enfant à l'autre, mais nous estimons qu'il y a un âge minimum sous lequel les jeunes enfants ne sont probablement pas en mesure de comprendre pleinement les conséquences de leurs choix concernant la protection de la vie privée, surtout à une époque où le flux des données est complexe. C'est pourquoi nous adoptons la position suivante : sauf dans les cas exceptionnels, le consentement à la collecte, à l'utilisation et à la communication de renseignements personnels d'enfants de moins de 13 ans doit être obtenu auprès des parents ou tuteurs.

2 *Banque Royale du Canada c. Trang*, 2016 CSC 50.

Pour ce qui est des jeunes âgés de 13 à 18 ans, le consentement peut être considéré comme valable uniquement si l'organisation a pris en compte leur degré de maturité et adapté en conséquence son processus de consentement. Nos lignes directrices provisoires sur le consentement proposeront une orientation à ce sujet.

Encourager l'utilisation de technologies visant à faciliter le processus de consentement

La technologie a un rôle à jouer lorsque les moyens traditionnels utilisés pour donner un consentement valable ont échoué. Elle pourrait faciliter le processus de consentement et le rendre plus pratique et valable. Plusieurs solutions techniques susceptibles d'améliorer le processus de consentement ont été discutées au cours des séances de consultation du Commissariat concernant le consentement et dans les mémoires présentés à ce sujet. À notre avis, les technologies et les bonnes idées pour faciliter ce processus ne manquent pas, mais le milieu des affaires ne semble pas les déployer ou les adopter. L'environnement économique et réglementaire actuel offre peu d'incitatifs au déploiement des technologies prometteuses visant à améliorer le processus de consentement, si bien que leur développement accru ne pourra probablement pas à lui seul entraîner des changements importants.

Pour sensibiliser le public aux technologies existantes visant à améliorer le processus de consentement et l'encourager à les utiliser, le Commissariat publiera du matériel éducatif recensant différentes technologies actuellement offertes sur le marché. Nous trouverons aussi des moyens de financer les activités de recherche et de transfert du savoir afin de promouvoir le développement des technologies visant à améliorer le processus de consentement et leur adoption par l'industrie grâce au Programme des contributions du Commissariat. Nous prévoyons aussi examiner les possibilités de jouer un rôle actif au sein des organismes de normalisation et des groupes sectoriels.

Nous estimons que les entreprises devraient aider les individus à prendre des décisions en matière de protection de la vie privée. Nous sommes particulièrement préoccupés par les déclarations selon lesquelles les entreprises pourraient se faire complices de l'établissement d'un environnement qui ne fait aucun cas de l'utilisation par les individus des technologies visant à améliorer le processus de consentement ou qui s'y oppose. Par exemple, on ne peut interrompre ni contrôler certains types de technologies de suivi utilisés dans la publicité comportementale en ligne sans avoir à prendre des mesures extraordinaires (et dans certains cas pas du tout). Il s'agit, par exemple, des témoins zombies, des supertémoins et de la prise d'empreintes numériques. À cette fin, nous encouragerons les individus à nous informer des problèmes rencontrés lorsqu'ils tentent d'utiliser ces nouvelles technologies et s'aperçoivent que, quoi qu'il en soit, leur choix n'est pas respecté. Nous étudierons les problèmes signalés si nous avons des raisons de croire que les choix en matière de protection de la vie privée des individus sont bafoués ou qu'ils sont modifiés contre leur gré. De manière générale, il y a place pour l'intervention de l'État dans le domaine. Dans le cadre de la stratégie gouvernementale pour promouvoir le développement et l'adoption de technologies novatrices, comme l'intelligence artificielle ou les supergrappes, nous encourageons le gouvernement à financer les technologies à la condition qu'elles intègrent des mesures de protection de la vie privée. À notre avis, c'est l'occasion pour lui de tirer parti de l'innovation et d'améliorer l'ensemble des mesures de protection de la vie privée.

Zones interdites même avec l'obtention du consentement

Entre autres questions, nous avons demandé aux intervenants s'ils jugent nécessaire de modifier la LPRPDE (ou toute autre loi) afin de prévoir des interdictions claires et précises quant à l'utilisation des renseignements personnels même après avoir obtenu le consentement (ce qu'on appelle les « zones interdites »). En vertu du paragraphe 5(3) de la LPRPDE, les utilisations inacceptables sont déjà interdites et le consentement ne permet pas de contourner l'interdiction, mais ces utilisations sont vastes et sujettes à interprétation.

Nous sommes d'accord avec les intervenants sur le fait qu'il ne serait pas idéal de prévoir dans la loi des zones interdites précises, compte tenu du rythme rapide des changements et de l'innovation. Nous avons cependant l'intention de publier un document d'orientation en vertu du paragraphe 5(3) afin de préciser aux organisations ce que nous considérons comme des utilisations inacceptables en nous plaçant du point de vue de la « personne raisonnable », ce qui, selon nous, sera également utile aux consommateurs. Nous diffuserons une version préliminaire de ce document d'orientation et demanderons des commentaires avant d'y mettre la touche finale. Notre première version se fonde sur les commentaires formulés pendant les consultations ainsi qu'à l'expérience que nous avons acquise au cours des 15 dernières années en faisant enquête sur les pratiques de protection de la vie privée et en écoutant les préoccupations des Canadiens. Voici quelques exemples de fins que, selon nous, une personne raisonnable n'estimerait pas acceptables : la collecte, l'utilisation ou la communication de renseignements qui autrement seraient illégales; un profilage ou une catégorisation donnant lieu à un traitement injuste, contraire à l'éthique ou discriminatoire; la publication de renseignements personnels dans le but de réclamer un paiement aux individus pour les retirer; et les situations qui risquent de causer un préjudice grave à l'intéressé . Par « préjudice grave », on entend les dommages matériels ou l'atteinte à la réputation au sens du nouveau paragraphe 10.1(7) de la LPRPDE, qui a été adopté, mais qui n'est pas encore en vigueur.

Bien que le droit à la vie privée puisse être violé sans qu'il y ait un préjudice, certains intervenants ont mentionné le rôle important du préjudice dans l'application de ce droit fondamental. Nous convenons que la réduction du risque de préjudice est l'un des objectifs des lois sur la protection des renseignements personnels et, comme il a déjà été mentionné, nous estimons qu'il faut en faire mention explicitement dans la loi. En particulier, lorsque l'on sait que la collecte, l'utilisation ou la communication de renseignements personnels cause un préjudice grave aux individus ou qu'elle est susceptible d'en causer un, elle devrait être prohibée. Par contre, lorsque le risque de préjudice est moindre et raisonnable en contrepartie d'un avantage, le choix de l'accepter ou de le refuser devrait revenir à l'individu. Pour que les décisions à cet égard soient éclairées, l'organisation doit être transparente dans la divulgation des risques et l'individu doit indiquer explicitement qu'il les accepte.

Orientations à l'intention des individus et des organisations

La protection de la vie privée repose en premier lieu sur le savoir. Pour l'individu, il s'agit de pouvoir cerner les risques d'atteinte à sa vie privée, d'avoir les compétences pour les atténuer et de savoir comment exercer son droit à la vie privée. Quant aux organisations, elles doivent connaître leurs obligations en matière de protection de la vie privée et comprendre ce que l'on attend d'elles avec une certaine uniformité et prévisibilité afin de respecter la loi.

Au cours des consultations sur le consentement, un très grand nombre d'intervenants ont demandé au Commissariat de renseigner et d'orienter davantage les individus et les organisations. Nous convenons que c'est un élément au cœur non seulement de la question du consentement, mais aussi d'une protection efficace de la vie privée dans son ensemble. Selon certains intervenants, les entreprises comptent sur le Commissariat pour élaborer et promouvoir des pratiques exemplaires en matière de protection de la vie privée ainsi que pour clarifier les exigences de la LPRPDE. Les documents d'orientation sont particulièrement utiles aux petites et moyennes entreprises, qui connaissent généralement moins bien la LPRPDE et qui manquent de ressources pour bien protéger la vie privée.

Les participants aux groupes de discussion souhaitent généralement avoir de l'information sur les questions relatives à la protection de la vie privée. Entre autres, ils veulent savoir quels sont les éléments importants d'une politique de confidentialité et quels sont les moyens de gérer les risques associés à la communication de renseignements personnels aux entreprises. Dans le cadre de son mandat d'éducation du public, le Commissariat est fermement déterminé

à faire connaître les questions relatives à la protection de la vie privée et à fournir de l'information aux individus pour les aider à exercer leur droit à cet égard et réduire le risque d'atteintes. L'éducation du public présente un avantage supplémentaire du fait qu'elle donne aux consommateurs le pouvoir de demander des comptes aux entreprises en posant des questions et en déposant des plaintes.

Il est toutefois important de reconnaître que l'éducation du public ne profite pas seulement aux consommateurs. Tous les Canadiens, quel que soit leur rôle dans l'économie, doivent acquérir des compétences numériques afin d'exercer leur droit à la vie privée et d'avoir le contrôle sur leurs renseignements personnels. Il faut tout particulièrement renseigner les enfants sur la protection de la vie privée et la valeur qu'elle représente pour les individus et la société afin de leur permettre de prendre des décisions éclairées.

L'accent particulier que met le Commissariat sur le matériel éducatif aide les enfants et les jeunes à acquérir les compétences dont ils ont besoin pour évaluer et atténuer les risques d'atteinte à la vie privée et faire des choix éclairés pour la protéger. À cette fin, nous avons conçu des ressources destinées aux parents, aux éducateurs et aux bibliothécaires, notamment des plans de cours, des fiches d'information et une bande dessinée afin de renseigner les enfants. Sur la scène internationale, nous avons participé à la rédaction de la résolution de Marrakech de 2016 réclamant l'adoption d'un référentiel de formation des élèves à la protection des données personnelles. À l'heure actuelle, dans le cadre du Groupe de travail international en éducation au numérique, nous participons aux efforts visant à favoriser l'acquisition de compétences en matière de protection des données et de la vie privée dans le programme scolaire des élèves du monde entier.

Nous sommes fiers du travail que nous avons accompli à ce jour dans le domaine, mais les limites de notre champ de compétence en tant qu'organisme fédéral restreignent notre capacité d'avoir une incidence sur l'éducation. Signalons que les commissaires provinciaux et territoriaux ont exprimé des préoccupations similaires concernant la nécessité d'améliorer l'éducation au numérique. Ensemble, nous demandons que l'éducation à la protection de la vie privée fasse partie intégrante du programme scolaire dès les premières années. Pratiquement tous les Canadiens reçoivent l'éducation de la maternelle à la 12e année et même si des programmes provinciaux abordent dans une certaine mesure les compétences liées à la protection de la vie privée, il ne faudrait pas négliger la nécessité de promouvoir l'acquisition de compétences dans le domaine de manière globale et cohérente. Nous sommes prêts à soutenir nos collègues provinciaux et territoriaux pour aider à institutionnaliser l'éducation à la protection de la vie privée. Les enfants auront ainsi les moyens de protéger leur vie privée dès leur jeune âge et seront prêts à prendre pleinement part au monde numérique en connaissant la valeur de la protection des renseignements personnels et en ayant les compétences voulues pour exercer leur droit à la vie privée.

Au-delà du programme scolaire, l'éducation et les orientations relatives à la protection de la vie privée à l'intention des individus sont au cœur de notre plan d'action pour accroître le contrôle qu'exercent sur leurs renseignements personnels les Canadiens de tous les groupes d'âge, y compris les personnes âgées. À cette fin, nous avons recensé une série de sujets liés à la vie privée sur lesquels il serait bon, d'après nous, de renseigner les Canadiens. Nous comptons publier des orientations et des fiches d'information dans le plus grand nombre de domaines possible afin d'aider les Canadiens à mieux comprendre les répercussions sur la vie privée et les outiller à exprimer leurs choix en la matière. Nous avons aussi cerné des sujets sur lesquels nous avons l'intention de diffuser des orientations ou de mettre à jour le matériel s'adressant aux entreprises afin d'aider à accroître la clarté et la certitude autour de questions ou de pratiques particulières :

1. Consentement (notamment les formes de consentement)
2. Zones interdites en vertu du paragraphe 5(3)
3. Désidentification

4. Mégadonnées, intelligence artificielle et robotique
5. Information génétique
6. Internet des objets
7. Véhicules connectés
8. Maisons intelligentes
9. Technologies renforçant la protection de la vie privée
10. Technologies de surveillance
11. Protection de la vie privée à la frontière (frontières intelligentes)
12. Nécessité et proportionnalité dans le secteur public
13. Réputation en ligne
14. Protection de la vie privée et médias sociaux
15. Applications et plateformes éducatives
16. Biométrie et reconnaissance faciale
17. Suivi sans témoins
18. Chaîne de blocs
19. Technologies numériques de la santé
20. Chiffrement de bout en bout
21. Ingénierie sociale
22. Circulation transfrontalière des données et infonuagique
23. Gouvernement ouvert
24. Modèle de maturité en matière de responsabilité
25. Avis d'incident
26. Courtiers en données
27. Technologie financière
28. Économie de partage
29. Suivi en magasin
30. Économie comportementale

Nous ne pouvons pas promettre de nous attaquer à tous les sujets figurant sur cette liste aussi rapidement que nous le voudrions, mais nous nous engageons à en traiter le plus possible d'ici 2021 en tenant compte de notre charge de travail et de nos ressources. Reconnaissant qu'il est impossible de tout faire dans un proche avenir, nous commencerons au cours des deux prochaines années par les domaines où nous observons les plus grands besoins directement liés aux enjeux soulevés dans le présent chapitre : le consentement en ligne, les zones interdites en vertu du paragraphe 5(3), la désidentification et les technologies renforçant la protection de la vie privée, l'information génétique et les avis d'incident. En outre, nous déploierons des efforts en parallèle sur le front de la réputation en ligne, de la biométrie et de la protection de la vie privée à la frontière et nous publierons des recherches sur l'intelligence artificielle.

Nous encouragerons également l'industrie à nous aider en élaborant des codes de pratique dans certains secteurs clés. Dans un premier temps, au moyen de notre Programme des contributions, nous finançons deux projets de recherche visant à établir des codes de pratique respectivement sur les véhicules connectés et les applications juridiques. Nous espérons poursuivre dans cette voie dans un avenir rapproché. Les codes de pratique constituent un outil utile et efficace pour accroître la conformité.

Mesures prévues par le Commissariat

- Le Commissariat publiera un document d'orientation mis à jour sur le consentement en ligne qui énoncera les attentes suivantes :
  - Les organisations doivent continuer de rendre facilement accessibles aux individus des renseignements complets et compréhensibles, mais, pour obtenir un consentement éclairé, il faut mettre de l'avant les éléments ci-après et les présenter au bon moment dans un format convivial :
    - quels renseignements personnels sont recueillis;
    - à qui ils sont communiqués;
    - à quelles fins les renseignements sont recueillis, utilisés ou communiqués, y compris une explication des fins non essentielles à la prestation du service;
    - quel est le risque de préjudice pour l'individu, le cas échéant.
  - Au moment de déterminer la forme du consentement, les organisations doivent prendre en compte les attentes raisonnables de l'individu, de la sensibilité des renseignements et du risque de préjudice.
- Le Commissariat modifiera aussi ses lignes directrices sur la responsabilité afin de préciser que les organisations doivent mettre l'accent sur quelques éléments d'information clés et pouvoir montrer qu'elles ont mis en place un processus permettant de vérifier si leur mécanisme de consentement fonctionne bien.
- Le Commissariat publiera un nouveau document d'orientation en vertu du paragraphe 5(3) de la LPRPDE (zones interdites) indiquant explicitement les cas de collecte, d'utilisation ou de communication de renseignements personnels que, selon lui, une personne raisonnable n'estimerait pas acceptables. Ce document fera ensuite l'objet d'une consultation.
- Le Commissariat définira mieux le concept d'attentes raisonnables des individus dans différents contextes, entre autres afin d'éclairer la forme de consentement.
- Le Commissariat informera les personnes des outils technologiques à leur disposition conçus pour mettre en œuvre leurs choix en matière de consentement et il se penchera sur les incidents qui lui auront été déclarés concernant des choix non respectés.
- Le Commissariat financera des activités de recherche et de transfert des connaissances au moyen de son Programme des contributions afin de promouvoir le développement et l'adoption de nouvelles technologies visant à améliorer le processus de consentement.
- Le Commissariat examinera les possibilités de jouer un rôle actif au sein des organismes de normalisation et des groupes de l'industrie afin de promouvoir les technologies visant à améliorer le processus de consentement.
- Le Commissariat diffusera des fiches d'information (documents d'information) dans le plus grand nombre de domaines possible afin d'aider les Canadiens à mieux comprendre les répercussions sur la protection des renseignements personnels et à exercer leur droit à la vie privée. De même, nous publierons à l'intention des organisations des documents d'orientation dans le plus grand nombre de domaines possible sur les mesures à prendre pour respecter leurs obligations en matière de protection de la vie privée.
- Le Commissariat encouragera l'industrie à élaborer des codes de pratique, en commençant par les véhicules connectés et les applications juridiques.

Recommandations du Commissariat

- Le Parlement devrait envisager de rendre le risque de préjudice explicite dans la LPRPDE, par exemple afin d'orienter la forme de consentement (implicite ou explicite).
- Le Commissariat encourage le gouvernement à financer les nouvelles technologies qui intègrent des mesures de protection de la vie privée afin d'aider à créer des incitatifs en vue de leur adoption.
- Le Commissariat enjoint aux gouvernements provinciaux et territoriaux d'intégrer l'éducation à la protection de la vie privée dans leurs programmes scolaires.

Solutions de remplacement du consentement

Quelles que soient les mesures prises pour faciliter le consentement et renforcer la capacité des individus à donner un consentement éclairé et celle des organisations à l'obtenir, il n'en demeure pas moins qu'il n'est tout simplement pas possible d'obtenir le consentement dans certaines situations. Ces situations sont probablement exceptionnelles, mais leur nombre pourrait s'accroître à mesure que la technologie évoluera. Tel que le précise le document de discussion sur le consentement et comme nous l'avons indiqué précédemment, les modèles d'affaires, facilités par les nouvelles technologies, ne se limitent plus du tout aux relations transactionnelles traditionnelles habituellement bilatérales envisagées au moment de la rédaction de la LPRPDE. Loin de là. Alors que l'on pouvait par le passé décrire les entreprises en fonction de leur principal secteur d'activité—vente au détail, télécommunications, divertissement, etc.—, bon nombre d'entre elles sont aujourd'hui devenues des sociétés de données multicanaux alimentées par les renseignements personnels. Dans certains cas, la technologie est devenue tellement complexe et les algorithmes tellement compliqués qu'il est quasiment impossible de comprendre comment sont gérés les renseignements personnels ou quelles peuvent être les conséquences, ce qui affaiblit la pertinence et la validité du consentement éclairé. Les innovations comme l'intelligence artificielle et la robotique ne pourront qu'accroître le degré de complexité dans l'avenir. Nous présentons ci-après trois solutions possibles pour renforcer les mesures de protection de la vie privée dans ce type de situations.

Désidentification

La désidentification a suscité un vif intérêt dans les tables rondes des intervenants, particulièrement auprès des représentants de l'industrie, qui y voient une façon d'atténuer les risques d'atteinte à la vie privée et de relever certains défis liés au consentement en vertu de la LPRPDE. Pourtant, certains participants ont aussi exprimé beaucoup d'inquiétudes concernant le risque de réidentification et la nécessité correspondante de procéder avec soin lorsqu'on précise à quel moment les exigences de la LPRPDE ne s'appliqueraient plus aux renseignements.

Compte tenu des grandes quantités de renseignements personnels traités dans l'environnement numérique, la désidentification peut sembler une mesure prometteuse pour renforcer la protection de la vie privée. Par ailleurs, nous reconnaissons les inquiétudes sur le fait que la réidentification présente un risque réel en raison non seulement de la disponibilité d'ensembles de données pouvant servir à repersonnaliser les renseignements personnels, mais aussi du manque de rigueur dans les méthodes de désidentification. Malgré tout, nous sommes d'un optimisme prudent—la désidentification pourrait être une solution viable pourvu qu'elle soit gérée correctement.

À cette fin, nous avons l'intention de publier un document d'orientation sur la désidentification, notamment pour aider les organisations à quantifier ce que l'on entend par un « risque grave de réidentification ». À l'heure actuelle, la loi énonce comme norme juridique la possibilité sérieuse d'identifier un individu à partir de données seules ou combinées avec d'autres et nous avons l'intention de définir les facteurs que nous estimons essentiels pour évaluer ce seuil, sur le plan qualitatif et quantitatif. Le document d'orientation aidera les organisations à évaluer le risque de réidentification et à le ramener à un niveau assez faible pour que les renseignements puissent être raisonnablement utilisés sans consentement.

Par ailleurs, nous jugeons utile l'idée de différents niveaux d'identifiabilité pouvant donner lieu à des exigences relatives à la protection de la vie privée plus ou moins rigoureuses selon le niveau de risque d'atteinte à la vie privée. Par exemple, le Règlement général sur la protection des données (RGPD) de

l'Union européenne reconnaît la pseudonymisation comme une mesure de protection qui donne aux organisations une souplesse accrue lors du traitement de renseignements pseudonymisés tout en continuant de considérer ces renseignements comme personnels aux fins de l'application de la loi.

En outre, d'éminents juristes et spécialistes de la protection de la vie privée se penchent actuellement sur l'idée que des catégories de données différentes allant au-delà du concept de blanc ou noir requièrent des niveaux de protection différents, plus ou moins rigoureux selon le risque de réidentification. Par exemple, un document présenté en 2016 au Symposium sur la protection de la vie privée de Bruxelles par El Emam et ses collaborateurs fait fond sur des travaux de recherche antérieurs afin de proposer un cadre de classification de l'état des données—entre les renseignements ne permettant pas d'identifier un individu et les renseignements personnels—en prenant en compte le risque d'identification et en proposant des méthodes d'atténuation du risque d'atteinte à la vie privée[3]. Nous encourageons le Parlement à examiner cette nouvelle question, qui pourrait assurer la souplesse nécessaire pour atteindre un meilleur équilibre entre la protection de la vie privée et la valeur économique des données.

Renseignements auxquels le public a accès

Dans le but de promouvoir un assouplissement des exigences concernant le consentement, certains intervenants de l'industrie ont suggéré des modifications au Règlement précisant les renseignements auxquels le public a accès. Ils soutiennent que les catégories de « renseignements auxquels le public a accès » doivent mieux refléter l'environnement d'aujourd'hui où les renseignements personnels peuvent être facilement accessibles dans les « espaces ouverts » comme Internet.

À notre avis, ce règlement d'application de la LPRPDE donne un aperçu ponctuel de ce que les législateurs considéraient comme des formes généralement acceptées de renseignements auxquels le public avait accès au tournant du siècle. Nous convenons qu'une mise à jour s'impose. Toutefois, nous faisons une mise en garde contre la fausse idée souvent véhiculée que les renseignements personnels ne présentent aucun intérêt sur le plan de la protection de la vie privée simplement parce qu'ils sont généralement accessibles en ligne.

La décision concernant la façon de protéger la vie privée des individus dont les renseignements sont accessibles au public est extrêmement complexe. Il faudra prendre en compte de nombreux éléments, dont les fins visées par les personnes qui affichent leurs propres renseignements personnels, et déterminer la façon de traiter les renseignements personnels affichés par des tiers. Elle soulève aussi des questions fondamentales relatives à la liberté d'expression et au droit d'accès à l'information dans l'intérêt public. Nous examinons actuellement ces questions dans le contexte de notre projet sur la réputation et pourrons peut-être en dire davantage plus tard cette année. Au bout du compte, vu l'importance de cet enjeu, une simple modification du règlement par le gouverneur en conseil ne serait cependant pas suffisante. Le sujet mérite plutôt que le Parlement l'étudie attentivement et en débatte, car ces questions doivent faire l'objet d'une réflexion approfondie; il faut pouvoir trouver un équilibre entre les droits fondamentaux l'individu et ceux de la société.

Nouvelles exceptions en matière de consentement

Les concepts de désidentification et de renseignements accessibles au public touchent la question du consentement dans une certaine mesure. Il reste toutefois des situations où l'obtention du consentement est tout simplement ou pratiquement impossible et on doit donc assurer autrement la protection de la vie privée. Certains intervenants ont fait valoir que la LPRPDE n'a jamais été censée s'appliquer à des activités où il n'y a aucune relation entre un individu et l'organisation qui recueille et

3 Khaled El Emam, Éloïse Gratton, Jules Polonetsky et Luk Arbuckle, *The Seven States of Data: When is Pseudonymous Data Not Personal Information?*, présenté au Symposium sur la protection de la vie privée tenu à Bruxelles en 2016.

utilise les renseignements personnels. Pourtant, ces situations soulèvent des questions relatives à la vie privée qu'il faut régler.

Par ailleurs, même dans certaines situations où une relation peut exister entre un individu et une entreprise, l'obtention du consentement pourrait être pratiquement impossible. C'est le cas, par exemple, dans le contexte des mégadonnées où d'énormes quantités de données sont recueillies en continu, où ces données peuvent servir à de nombreuses fins nouvelles et où les algorithmes sont si complexes qu'il est difficile de les expliquer de façon à ce que les consommateurs puissent les comprendre. Dans certaines situations, il est possible de demander le consentement à des fins nouvelles et on doit alors le faire. Cependant, nous estimons aussi qu'il serait probablement non seulement difficile, mais aussi pratiquement impossible d'obtenir un nouveau consentement dans certains cas.

Nous encourageons le Parlement à déterminer s'il pourrait être approprié de prévoir de nouvelles exceptions à l'obligation d'obtenir un consentement lorsque ce n'est simplement pas possible ni réaliste.

Pour surmonter ces difficultés, nous suggérons que le Parlement envisage de modifier la LPRPDE pour prévoir à l'article 7 de nouvelles exceptions en matière de consentement permettant des activités bénéfiques pour la société que les rédacteurs initiaux de la LPRPDE n'avaient pas envisagées. La recommandation d'intégrer ces types d'exceptions peut sembler contraire à notre mission en tant qu'organisme de réglementation de la protection de la vie privée, mais nous en sommes venus à la conclusion qu'il est préférable de reconnaître cette réalité et d'adopter des mesures de protection appropriées plutôt que d'étirer ou de déformer le concept du consentement implicite au point de lui faire perdre sa pertinence.

De telles exceptions en matière de consentement devraient se limiter aux situations où les avantages pour la société l'emportent manifestement sur les ingérences dans la vie privée et plusieurs conditions préalables devront être remplies avant que les renseignements puissent servir à ces fins. Nous recommandons au Parlement d'examiner les situations où ces exceptions seraient justifiées dans une perspective sociale globale. À notre avis, les situations où l'obtention du consentement est pratiquement impossible incluent : indexation des sites Web par les moteurs de recherche et présentation des résultats de recherche aux internautes, s'il y a lieu; services de géolocalisation sur lesquels la société compte de plus en plus; ou certains processus de traitement de données tels que l'analyse des mégadonnées, l'Internet des objets, l'intelligence artificielle ou les applications robotiques lorsqu'il y a concordance des intérêts commerciaux et sociaux.

En ce qui a trait aux conditions préalables imposées, une organisation pourrait avoir à montrer sur demande ce qui suit :

- il est nécessaire d'utiliser les renseignements personnels;
- il est pratiquement impossible d'obtenir le consentement;
- des données pseudonymisées seront utilisées dans la mesure du possible;
- les avantages sociétaux l'emportent manifestement sur les ingérences dans la vie privée;
- une évaluation des facteurs relatifs à la vie privée 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.

Il serait possible de prévoir une exception générale liée à « l'intérêt légitime » comme c'est le cas dans le RGPD de l'Union européenne (et, depuis quelque temps déjà, dans certaines lois nationales), mais nous pensons qu'il serait préférable que les exceptions prennent la forme d'une liste de situations particulières, comme celles susmentionnées. Il en serait ainsi pour deux raisons : premièrement, le concept d'intérêts légitimes est très large et peut regrouper plusieurs situations où une exception en matière de consentement n'est pas nécessaire; deuxièmement—dans le même ordre d'idées –, il existe un risque que les organisations abusent de ce nouveau concept et le considèrent comme une autorisation générale de recueillir, d'utiliser ou de communiquer des renseignements personnels, même si la liste de conditions à respecter ci-dessus atténuerait ce risque.

On devrait pouvoir invoquer ces exceptions uniquement en dernier recours après avoir examiné toutes les façons possibles d'obtenir le consentement et constaté que ces mesures sont pratiquement impossibles. De plus, une nouvelle exception en matière de consentement devrait nécessairement reposer sur des pouvoirs d'application de la loi renforcés (voir ci-après) permettant aux organismes de réglementation de la protection de la vie privée, s'il y a lieu, de déterminer si l'utilisation des renseignements personnels sert des fins sociales globales et remplit les conditions prévues par la loi. Précisons que cette démarche ne s'inscrirait pas dans le cadre d'un régime d'autorisation préalable, mais qu'elle ferait plutôt appel au type de modèle d'application proactive de la loi que nous proposons ci-après.

Mesures prévues par le Commissariat

- Le Commissariat publiera un document d'orientation proposant des méthodes de désidentification appropriées et recensant les facteurs à prendre en compte dans l'évaluation, aussi bien qualitative que quantitative, lorsque le risque de réidentification sera assez faible pour que l'on autorise l'utilisation des renseignements sans consentement.

Recommandations du Commissariat

- Le Parlement devrait examiner la possibilité de prévoir de nouvelles exceptions en matière de consentement pour gérer les activités où les avantages pour la société l'emportent manifestement sur les ingérences dans la vie privée, sous réserve de conditions strictes et de pouvoirs d'application de la loi renforcés.
- Le Parlement devrait examiner le concept des renseignements pseudonymisés, qui pourraient être soustraits aux exigences relatives au consentement tout en demeurant assujettis à toutes les autres mesures de protection prévues par la LPRPDE.
- Le Parlement devrait déterminer la meilleure façon de moderniser le *Règlement précisant les renseignements auxquels le public a accès* en prenant en compte la nécessité d'assurer un équilibre entre des droits constitutionnels potentiellement concurrents.

Gouvernance

La section précédente énonçait des façons d'adapter le modèle de consentement afin de surmonter les difficultés inhérentes à un environnement riche en données numériques. La présente porte sur les mécanismes qui permettront aux entreprises de mettre en œuvre et de respecter les obligations leur incombant en vertu de la LPRPDE.

Responsabilité

La responsabilité est un principe fondamental énoncé dans la LPRPDE qui oblige les organisations à élaborer et à mettre en œuvre des politiques et des pratiques visant à faire respecter les principes de l'annexe 1 de la Loi. Collectivement, ces politiques et ces pratiques devraient constituer un programme cohérent de gestion de la protection de la vie privée. Certains participants aux consultations ont affirmé que la responsabilité devrait occuper une place plus importante.

Comme l'indique le document d'orientation conjoint sur la responsabilité publié par le Commissariat, ce dernier dispose du pouvoir implicite d'obliger les organisations à montrer qu'elles respectent les obligations énoncées au principe 4.1 de la LPRPDE dans le cadre d'une enquête ou d'une vérification. L'absence de politiques et de procédures démontrables en matière de protection de la vie privée a été invoquée dans de récentes enquêtes menées en vertu de la LPRPDE, notamment l'affaire Ashley Madison.

Le Commissariat n'a cependant pas le pouvoir de demander de façon purement proactive aux organisations de montrer qu'elles sont responsables. Le nouveau pouvoir d'examiner sur demande les dossiers d'incidents constitue un pas important dans cette direction—et nous nous en réjouissons –, mais ce n'est pas suffisant. Nous sommes convaincus que le Commissariat pourra assurer efficacement la conformité à la LPRPDE uniquement si les organisations sont tenues de montrer qu'elles sont responsables, non seulement après un incident malheureux, mais aussi de façon proactive. Nous profitons de l'occasion pour réitérer notre recommandation selon laquelle le gouvernement devrait envisager de remédier à la situation en modifiant la LPRPDE.

Comme il en est question dans le document d'orientation sur la responsabilité, le but d'un programme de gestion de la protection de la vie privée est d'aider les organisations à intégrer la protection de la vie privée dès la conception d'un produit ou d'un service—depuis la conception initiale jusqu'à la mise en œuvre et au déploiement et par la suite. Comme nous l'avons déjà mentionné, les intervenants sont généralement favorables à la protection de la vie privée dès la conception (concept préconisé par Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario), mais ils ne jugent pas nécessaire d'en faire une exigence explicite en vertu de la loi. Ils font valoir que le concept y figurait déjà implicitement et qu'il ne devrait pas devenir trop normatif. Deux éléments de la protection de la vie privée dès la conception qui nous semblent particulièrement importants sont les exigences temporelles (le plus rapidement possible et évaluation continue) et le fait que le concept englobe les facteurs technologiques et organisationnels. Ces deux éléments sont énoncés dans notre document d'orientation. Selon nous, ils sont tous les deux essentiels et nous nous attendons à ce qu'ils soient mis en œuvre. Pour aider les petites entreprises à s'acquitter de leurs obligations à ce chapitre, nous publierons une version modifiée de notre document d'orientation sur la responsabilité à l'intention des petites et moyennes entreprises et les aiderons à suivre un modèle de maturité en la matière à mesure qu'elles prendront de l'expansion.

Par ailleurs, pour les besoins de la responsabilité, nous considérons que les organisations doivent pouvoir montrer les mesures prises volontairement

afin de concevoir et de mettre en œuvre un processus de consentement éclairé que le public cible pourra comprendre et qui sera adapté à la nature de leur produit ou service. Nous avons mis à jour le document d'orientation sur le consentement en ligne afin de clarifier les attentes et accueillons favorablement tout commentaire à ce sujet.

En ce qui concerne l'utilisation des marques de confiance comme autre façon de montrer de manière proactive qu'une organisation est responsable, les participants n'étaient généralement pas favorables à cette pratique en raison de l'expérience à ce jour. De nombreux intervenants se méfient des programmes de marques de confiance conçus et mis en œuvre par l'industrie pour l'industrie, invoquant l'absence d'indépendance comme une préoccupation majeure. Quelques participants se sont cependant dits favorables aux marques de confiance supervisées par une organisation indépendante crédible, comme le Bureau d'éthique commerciale ou le Commissariat. Signalons que le Canada participe au régime des Règles transfrontalières de protection de la vie privée (RTPVP) de Coopération économique Asie-Pacifique (APEC). Dans le cadre de ce régime volontaire, un tiers appelé « agent de vérification de la conformité » examine les politiques et les procédures de protection de la vie privée dans un contexte transfrontalier adoptées par les organisations qui souhaitent participer aux économies membres de l'APEC. Il certifie qu'elles respectent un ensemble d'exigences du programme fondées sur les principes du Cadre de protection de la vie privée de l'APEC. Un avis de la *Gazette du Canada* à l'intention des agents de vérification de la conformité selon les RTPVP a été affiché en décembre 2016 et nous surveillons avec intérêt l'évolution de la situation.

Éthique

Les intervenants sont généralement d'avis que la notion de comités d'éthique indépendants, empruntée au contexte de la recherche universitaire, se transpose mal dans le monde des affaires. Nous considérons néanmoins qu'il est important et utile de discuter l'intégration d'une perspective éthique dans la protection de la vie privée. Particulièrement en raison des conséquences discriminatoires possibles des mégadonnées et des répercussions encore inconnues sur la sécurité et la société des dispositifs de l'Internet des objets et des accessoires connectés à porter sur soi. Sans mentionner les conséquences de l'intelligence artificielle et de la robotique sur la société et l'humanité dans son ensemble. Nous reconnaissons toutefois que l'intégration de l'éthique dans les lois sur la protection de la vie privée, sous la forme de comités d'éthique assurant la protection des consommateurs ou autrement, n'est pas encore suffisamment avancée pour être pratique à court terme. Nous continuerons de suivre de près l'évolution de ce dossier et nous nous attachons à stimuler le débat sur ces questions quand l'occasion se présentera.

Application de la loi

Le Commissariat a publié en 2013 un document expliquant pourquoi une réforme de la LPRPDE s'imposait, faisant état des grands changements suscités par la technologie au cours des quelques années écoulées depuis l'entrée en vigueur de la LPRPDE et soulignant que des mesures plus robustes étaient nécessaires pour amener les organisations à intégrer des mesures de protection de la vie privée dès le départ. Nous avions alors prôné un renforcement des pouvoirs d'application de la loi pour créer ces mesures incitatives—le besoin est encore plus grand en 2017. La technologie continue d'évoluer à un rythme sans précédent et, depuis la dernière fois que nous avons fait valoir nos arguments en faveur de l'examen de la LPRPDE. Les nouveaux services et les nouvelles entreprises ont tellement évolué que nous constatons maintenant la nature révolutionnaire des nouvelles technologies et des économies axées sur les données qui en étaient à leurs débuts au moment de l'adoption de la LPRPDE. L'économie dite de partage, l'Internet des objets, l'intelligence artificielle et la réalité amplifiée sont des exemples des technologies et services nouveaux appelés à modifier radicalement le mode d'interaction des Canadiens avec les entreprises et les machines ainsi qu'entre eux. Les renseignements personnels sont le nouveau prix à payer pour participer à ces économies.

À notre avis, le temps est venu pour le Canada de modifier son modèle réglementaire pour s'assurer que, tout comme aux États-Unis, au sein de l'Union européenne et ailleurs, ses organismes de réglementation peuvent protéger efficacement le droit à la vie privée de ses citoyens en étant dotés de pouvoirs d'intervention importants et proportionnels au risque croissant d'atteinte à la vie privée que présentent les nouvelles technologies révolutionnaires.

Le moment est venu pour le Canada de modifier son modèle de protection de la vie privée afin de s'assurer que, tout comme aux États-Unis, au sein de l'Union européenne et ailleurs, ses organismes de réglementation peuvent protéger efficacement le droit à la vie privée de ses citoyens en ayant des pouvoirs proportionnels au risque croissant d'atteinte à la vie privée que présentent les nouvelles technologies révolutionnaires.

Les Canadiens nous ont dit qu'ils sont inquiets—92 % des répondants à notre sondage sont préoccupés au sujet de la protection de leur vie privée. Les participants des groupes de discussion sont largement en faveur de l'idée que le gouvernement contrôle les entreprises pour s'assurer qu'elles respectent les lois sur la protection des renseignements personnels. Ils sont d'accord avec une application de la loi à la fois proactive et réactive. Le point de vue des membres des groupes de discussion concorde, dans une large mesure, avec les résultats de notre récent sondage d'opinion, d'après lequel 69 % des Canadiens souhaitent que le commissaire ait le pouvoir de rendre des ordonnances pour faire appliquer les recommandations formulées à l'issue d'une enquête. De plus, 70 % des répondants seraient plus disposés à faire affaire avec une entreprise qui s'exposerait à de lourdes pénalités financières si elle utilisait leurs renseignements personnels à mauvais escient.

La LPRPDE a été « adoptée pour atténuer les inquiétudes des consommateurs concernant le respect de la vie privée et pour permettre au milieu des affaires canadien de soutenir la concurrence dans l'économie numérique mondiale[4] ». Elle avait pour objectif stratégique de renforcer la confiance dans le commerce électronique[5]. Ces objectifs sont aussi pertinents aujourd'hui qu'ils l'étaient à l'époque. Toutefois, les Canadiens ne se sentent pas protégés par une loi qui n'a pas de mordant et des organisations qui ne sont assujetties qu'à des recommandations non contraignantes.

D'autres gouvernements sont allés de l'avant pour conférer à leur autorité de protection des données le pouvoir d'accorder des dommages-intérêts, d'imposer des amendes et d'ordonner à une organisation de modifier ses pratiques ou de communiquer des renseignements personnels à un individu qui le demande. À l'échelle provinciale, les lois sur la protection des renseignements personnels dans le secteur privé en Alberta, en Colombie-Britannique et au Québec et la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario confèrent le pouvoir général de rendre des ordonnances, contrairement à la LPRPDE. Sur la scène internationale, bon nombre des principales lois sur la protection des données, notamment le *Règlement général sur la protection des données* (RGPD) et les lois sur la protection des données du Royaume-Uni et de l'Irlande, confèrent le pouvoir de rendre des ordonnances. Alors qu'aucune de nos lois provinciales ne donne au commissaire le pouvoir d'imposer des pénalités financières, les amendes ou les règlements financiers deviennent de plus en plus la norme sur la scène internationale. Dans le cadre du RGPD, les amendes s'élèvent à 4 % du chiffre d'affaires annuel de l'organisation; aux États-Unis, la Federal Trade Commission (FTC) a imposé des sanctions de 20 millions de dollars ou plus sous la forme d'accords de règlement; au Canada, la *Loi sur la concurrence* prévoit des sanctions administratives pécuniaires pouvant atteindre 15 millions de dollars selon divers

4 Site Web d'Industrie Canada, Commerce électronique au Canada – Protection des renseignements en affaires.

5 Notes pour une allocution de l'honorable John Manley devant le Comité sénatorial chargé d'étudier le projet de loi C-6, 2 décembre 1999.

facteurs. Le Canada a besoin de pouvoirs comparables à ceux conférés dans d'autres pays pour ce qui est de rendre des ordonnances et la possibilité d'imposer des amendes pour avoir une incidence réelle sur la protection de la vie privée et continuer de profiter des partenariats commerciaux établis avec l'Europe et d'autres parties. De plus, les lacunes en matière de pouvoirs de réglementation et d'application de la loi pourraient être un facteur déterminant au moment de l'examen par l'Union européenne du statut du Canada concernant le caractère adéquat de la protection.

Des intervenants de l'industrie considèrent qu'un renforcement de l'application de la loi étoufferait l'innovation et nuirait à la bonne relation de travail qu'entretient actuellement le Commissariat avec les organisations, relation qui produit des résultats positifs pour la protection de la vie privée. Ils estiment aussi qu'il n'est pas nécessaire de renforcer les pouvoirs d'application de la loi puisque les entreprises cherchent généralement à s'y conformer et que le Commissariat réussit très bien à ramener les contrevenants à l'ordre grâce aux outils existants—par exemple la diffusion des conclusions dans les cas de non-conformité.

Nous convenons que de nombreuses entreprises s'efforcent de se conformer à la LPRPDE, mais ce n'est pas le cas de toutes. Or, les recommandations et la peur d'une mauvaise presse ne permettent pas de ramener à l'ordre toutes les organisations récalcitrantes. Il faut protéger les consommateurs contre les « mauvais élèves » et les pratiques illégales adoptées par des organisations généralement responsables qui dépassent parfois les limites établies. Un renforcement de l'application de la loi peut aussi inciter les dirigeants d'entreprise à mettre l'accent sur la protection de la vie privée et à investir dans le domaine. Des intervenants ont affirmé que les entreprises canaliseront leurs ressources en matière de conformité vers les aspects où le risque est le plus grand. Ainsi, la menace de sanctions les inciterait à adopter des pratiques conformes à la LPRPDE. Par conséquent, les entreprises écouteront probablement davantage les organismes de réglementation comme la FTC que le Commissariat. Le fait que la FTC impose régulièrement des pénalités financières se chiffrant dans les millions de dollars ne semble pas avoir freiné l'innovation aux États-Unis.

Nous sommes conscients cependant que l'on devra déterminer avec soin et réflexion les facteurs pour imposer une sanction afin de mettre en évidence l'objectif ultime : améliorer la conformité plutôt que sévir. De cette façon, la LPRPDE serait semblable à plusieurs régimes de réglementation canadiens de longue date, et la diligence raisonnable (preuve qu'une organisation a pris toutes les mesures raisonnables pour éviter l'infraction constatée par l'organisme de réglementation) constituerait une défense complète exonérant l'organisation d'avoir à payer une sanction administrative pécuniaire. Le Parlement pourrait aussi imposer des facteurs à prendre en compte au moment de déterminer le montant des sanctions, par exemple selon qu'une organisation a mis en place les mesures de protection appropriées ou qu'elle peut faire la preuve d'un solide programme de protection de la vie privée ou, à l'inverse, qu'il y a récidive, insouciance ou violation flagrante.

Nous sommes d'avis que le modèle canadien fondé sur les plaintes et en grande partie réactif a connu un certain succès dans le passé, mais il fait face à des défis de taille à l'ère numérique. Et notre modèle de l'ombudsman ne nous a pas permis de donner aux Canadiens l'assurance que leur vie privée est protégée et qu'ils ont leur mot à dire sur ce qu'il advient de leurs renseignements personnels. L'objectif de la

Nous sommes convaincus que l'effet combiné d'une application de la loi proactive et d'une obligation de faire preuve de responsabilité serait beaucoup plus susceptible d'assurer la conformité à la LPRPDE et le respect du droit à la vie privée que le modèle actuel de l'ombudsman. Ceci requiert des changements urgents.

LPRPDE, énoncé à l'article 3, consiste à trouver un équilibre entre le droit des individus à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins raisonnables et acceptables. Pour atteindre cet objectif, le Parlement a choisi des mesures de surveillance particulières qui figurent principalement dans le modèle réactif de l'ombudsman. Ces mesures étaient pertinentes au moment de l'adoption de la LPRPDE, mais nous estimons que ce modèle ne permet plus de réaliser l'objectif global de la Loi.

En premier lieu, un système fondé sur les plaintes ne donne pas une image complète des failles possibles en matière de protection de la vie privée. Les plaintes déterminent les problèmes sur lesquels se penche le Commissariat et il s'agit souvent de préoccupations ponctuelles reposant sur l'expérience d'un seul individu qui ne reflète peut-être pas la réalité globale. Il est peu probable que les individus déposent une plainte pour dénoncer un fait dont ils n'ont pas conscience. Et à l'ère des mégadonnées et de l'Internet des objets, on peut très difficilement savoir et comprendre ce qu'il advient de nos renseignements personnels. En revanche, le Commissariat est mieux placé pour examiner les flux de données souvent obscurs et déterminer s'ils sont conformes à la LPRPDE.

C'est en partie pourquoi nous considérons que le modèle canadien devrait devenir plus proactif. Le commissaire à la protection de la vie privée a déjà le pouvoir de prendre l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question[6]. Cependant, contrairement à ses collègues du Royaume-Uni et de la France, il n'a pas le pouvoir de vérifier la conformité sur demande à moins d'avoir de motifs de croire qu'une infraction a été commise. Ces pouvoirs sont fréquents dans la réglementation canadienne, notamment en ce qui concerne les normes d'emploi, la santé et la sécurité, l'alimentation et les restaurants, le tabac et les valeurs mobilières.

En ce qui concerne le rôle du gouvernement dans la protection des renseignements personnels, la vaste majorité des participants de groupes de discussion conviennent qu'il devrait être à la fois proactif et réactif.

Un modèle proactif d'application de la loi serait le plus efficace pour s'assurer que les organisations puissent démontrer leur respect du principe de la responsabilité à l'égard de la protection de la vie privée des consommateurs. Tout au long de nos consultations, les intervenants ont souvent indiqué que la responsabilité devait occuper une place plus importante dans la protection de la vie privée, à une époque où les flux de données et les modèles d'affaires deviennent de plus en plus complexes, ce qui crée des difficultés pour l'application du modèle de consentement. Tout en considérant que le consentement joue toujours un rôle important, nous convenons qu'il faudrait accroître l'importance accordée à la responsabilité. Par conséquent, les organisations devraient avoir à démontrer sur demande qu'elles respectent le principe de responsabilité et ainsi qu'elles respectent le droit à la vie privée.

Pour l'instant, nous continuerons d'examiner des moyens de promouvoir de manière plus proactive la conformité à la LPRPDE dans le cadre du régime législatif actuel. Les activités proactives de conformité et d'application de la loi que nous envisageons actuellement sont l'exercice plus stratégique et fréquent des pouvoirs formels, notamment notre capacité de mener des enquêtes à l'initiative du commissaire conformément au paragraphe 11(2) de la

6 Paragraphe 11(2) de la LPRPDE.

Loi, ainsi que des enquêtes à l'échelle de secteurs afin d'atténuer les risques systémiques d'atteinte à la vie privée des Canadiens. Nous nous efforcerons aussi de donner des conseils aux organisations.

Les activités proactives de conformité et d'application de la loi peuvent toutefois nécessiter des ressources considérables. En outre, il serait difficile d'être beaucoup plus actifs dans le cadre de cette stratégie tout en menant des enquêtes sur presque toutes les plaintes déposées par des individus. Une solution consisterait à augmenter légèrement les ressources afin de pouvoir réaliser des activités de conformité aussi bien réactives que proactives. Une autre solution serait de renforcer notre pouvoir discrétionnaire pour décider quelles plaintes individuelles feront l'objet d'une enquête et lesquelles ne devraient pas être enquêtées afin de permettre au Commissariat de procéder à des examens proactifs systémiques susceptibles d'avoir une plus grande incidence positive sur les Canadiens. Nous privilégions la première des deux options. Toutefois, sans une augmentation modeste des ressources requises à cette fin, nous recommandons avec réticence d'accroître notre pouvoir discrétionnaire de refuser des plaintes individuelles pour nous permettre de réaffecter des ressources limitées à des activités de conformité davantage proactives et de produire les résultats qui, d'après ce que nous en sommes venus à croire, seraient plus percutants et durables pour les Canadiens. Nous déterminerions les critères de refus de plaintes qui tiendraient compte, par exemple, du fait que la plainte est ponctuelle ou de nature systémique et que l'individu dispose ou non d'autres options pour en arriver à une solution équitable.

Pour éviter que les individus se trouvent sans recours, le Parlement devrait à notre avis envisager de créer une forme de recours judiciaire, comme un droit privé d'intenter une action en justice dans les cas d'infraction à la LPRPDE, en vertu duquel les individus peuvent tout de même s'adresser aux tribunaux lorsque le Commissariat ne fait pas enquête ou qu'il ne produit pas de rapport de conclusions.

À notre avis, le temps est venu d'offrir aux individus l'option d'un accès direct à un recours judiciaire, probablement sous la forme d'un droit privé d'intenter une action en justice fondé sur les infractions à la Loi. Cette mesure pourrait être utile en servant à comprimer ce qui autrement serait une longue période de développement du droit de la responsabilité délictuelle appliquée à la protection de la vie privée et constituerait un outil complémentaire d'application de la loi et une solution de remplacement du modèle actuel fondé sur les plaintes. Nous reconnaissons toutefois que pour diverses raisons, notamment des questions de coût, de temps et d'accès, un droit privé d'intenter une action en justice ne constituera pas dans tous les cas une solution satisfaisante pour remplacer le régime actuel de plaintes. Nous tiendrions compte de cet aspect au moment de décider comment exercer notre pouvoir discrétionnaire de refuser une plainte.

Signalons que le gouvernement a récemment suspendu la mise en œuvre de certaines dispositions de la *Loi canadienne anti-pourriel* (LCAP), qui auraient créé un droit privé d'intenter une action en justice en cas d'infraction alléguée à cette loi. Il a agi ainsi parce que, d'une part, les Canadiens ont droit à une loi efficace, tandis que, d'autre part, les organisations assujetties à cette loi ne devraient pas avoir à subir des formalités administratives et des coûts inutiles afin de s'y conformer.

Nous comprenons l'appel à l'équilibre lancé par le gouvernement et sommes d'avis qu'il serait possible d'ajouter une forme de recours judiciaire sous le régime de la LPRPDE, comme un droit privé d'intenter une action en justice en toute indépendance, d'une manière qui permet d'atteindre cet équilibre. Les derniers développements en droit canadien de la responsabilité délictuelle semblent indiquer que le fait d'accorder aux individus un

droit privé d'intenter une action en justice pour les infractions à la LPRPDE constituerait une évolution raisonnable du régime canadien de protection des renseignements personnels dans le secteur privé. Selon nous, contrairement à certaines préoccupations concernant les formalités administratives exprimées dans le contexte de la LCAP, un accès plus direct au recours judiciaire pourrait dans certains cas simplifier l'accès à une réparation efficace en cas d'infraction à la Loi.

Mesures prévues par le Commissariat

- Le Commissariat continuera d'appliquer le principe du respect de la vie privée dès la conception d'un produit ou d'un service grâce à ses lignes directrices en matière de responsabilité et au principe de responsabilité énoncé dans la LPRPDE.
- Le Commissariat entend adapter son cadre de responsabilité actuel aux besoins des petites et moyennes entreprises et contribuer à orienter leur évolution au fur et à mesure qu'elles croîtront et gagneront en maturité.
- Le Commissariat recourra plus fréquemment et de façon plus stratégique à ses pouvoirs pour mener des enquêtes axées sur des problèmes chroniques ou sectoriels, ou d'autres problèmes liés à la protection de la vie privée en lien avec des modèles d'affaires ou des utilisations des renseignements personnels non transparents.

Recommandations du Commissariat

- Le gouvernement devrait modifier la LPRPDE pour :
  - imposer une exigence concernant l'obligation de démontrer le respect du principe de la responsabilité;
  - conférer au commissaire le pouvoir de rendre des ordonnances et la possibilité d'imposer des sanctions administratives pécuniaires;
  - conférer au commissaire le pouvoir d'effectuer des examens de conformité sur demande, sans avoir de motifs de croire qu'une infraction à la LPRPDE a été commise;
  - donner au commissaire le choix de faire enquête ou non sur les plaintes individuelles, afin de canaliser les ressources limitées vers les questions qui posent le risque le plus élevé pour les Canadiens ou qui peuvent avoir la plus grande incidence sur eux;
  - accorder aux personnes un droit privé d'intenter une action en justice en cas d'infraction à la LPRPDE.

Conclusion et prochaines étapes

Le consentement demeure au cœur de l'autonomie personnelle. Toutefois, afin que la vie privée soit protégée plus efficacement, il doit être soutenu par d'autres mécanismes, notamment les organismes de réglementation indépendants.

En formulant ces recommandations et l'orientation proposée, nous souhaitons nous assurer que le consentement donné par les individus est réellement valable. Nous encourageons les organisations à adopter une approche novatrice pour obtenir le consentement, à mieux exploiter la technologie pour désidentifier les renseignements et à faire preuve de responsabilité dans la protection des renseignements personnels tout au long de leur cycle de vie. Nous recommandons au Parlement et au gouvernement de se pencher sérieusement sur l'intérêt d'apporter certaines modifications et de mettre en place un cadre rigoureux d'application de la loi pour protéger les renseignements personnels des Canadiens au 21e siècle et aider à maintenir leur confiance dans l'économie numérique.

ÉTUDE DE LA LPRPDE

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) définit les règles de base régissant la gestion des renseignements personnels dans le secteur privé. Elle établit un équilibre entre le droit d'un individu à la protection de ses renseignements personnels et la nécessité pour les organisations de recueillir, d'utiliser ou de communiquer ces renseignements à des fins opérationnelles légitimes. Son entrée en vigueur en 2001 a marqué une étape importante dans la protection des renseignements personnels des Canadiens, mais elle est maintenant dépassée par la technologie à de nombreux égards. Même si un examen antérieur de la Loi a permis d'y apporter quelques modifications, l'évolution rapide de la technologie entraîne des changements dont l'ampleur remet en cause l'efficacité de la Loi et sa viabilité en tant qu'instrument de protection de la vie privée des Canadiens.

Conseils au Parlement

Comme dans le cas de la *Loi sur la protection des renseignements personnels*, le Commissariat préconise depuis plusieurs années la modernisation de la LPRPDE. Ainsi, nous étions heureux que le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes entreprenne une étude de la Loi en février 2017.

Nous ne remettons nullement en question les avantages considérables que les progrès dans les technologies de l'information et des communications procurent aux individus. En plus de faciliter grandement les communications, les nouvelles technologies donnent un large accès à des renseignements de toutes sortes ainsi qu'à des produits et services venant du monde entier, mais elles créent aussi des risques importants. Les internautes veulent exprimer leur opinion et faire des recherches sur des questions sensibles comme la santé sans craindre que quelqu'un suive ces activités et en fasse part à des tiers ayant des intérêts opposés aux leurs.

Avant le lancement de l'étude par le Parlement, dans une lettre adressée au Comité, le commissaire à la protection de la vie privée a soulevé plusieurs préoccupations concernant la législation actuelle et a proposé quatre grands enjeux comme domaines d'intervention possibles pour l'étude. Le commissaire a repris ces sujets—consentement, réputation, pouvoirs d'application de la loi et caractère adéquat—au cours d'une comparution devant le Comité.

Dans ses messages au Comité, le commissaire a fait état des travaux du Commissariat sur la réputation, qui sont présentés plus en détail ci-après. En ce qui a trait au consentement, il a parlé de la nécessité de moderniser le modèle actuel et a indiqué qu'il déposerait prochainement son rapport sur le sujet. Quant aux pouvoirs d'application de la loi, le commissaire a insisté sur les défis associés à des pouvoirs limités et a fait valoir qu'une approche axée davantage sur la conformité proactive s'impose.

Le commissaire a également rappelé au Parlement l'incidence de l'entrée en vigueur en 2018 du *Règlement général sur la protection des données* (RGPD) sur le territoire de l'Union européenne (UE) et l'examen du caractère adéquat du Canada. L'UE a signalé que le statut attribué au Canada est « partiel », c'est-à-dire qu'il s'applique uniquement à la LPRPDE, et que toutes les décisions à venir concernant le caractère adéquat reposeront sur une évaluation exhaustive du régime de protection de la vie privée du pays. Cette évaluation portera notamment sur l'accès des autorités publiques aux données personnelles aux fins de l'application de la loi, de la sécurité nationale et d'autres objectifs d'intérêt public. Compte tenu de l'incidence considérable sur le commerce et des différences entre le Règlement général et la LPRPDE,

il sera important que le Comité prenne cet aspect en considération lorsqu'il poursuivra son étude.

Nous serions heureux de formuler d'autres commentaires et avis à l'intention du Comité à mesure que son étude progressera. En particulier, nos recherches et nos analyses approfondies portant sur des enjeux comme le consentement et la réputation aideront à éclairer les recommandations concernant la modernisation de la LPRPDE que nous présenterons au Parlement, entre autres les modifications législatives recommandées dans la section du présent rapport portant sur le consentement à la page 13.

Réputation

Les Canadiens reconnaissent les avantages personnels et professionnels liés à leur participation au monde numérique, mais ils se préoccupent de plus en plus de leur réputation en ligne. D'une part, les gens veulent avoir une présence en ligne et croient que le fait de bien choisir ce qu'ils publient contribuera à forger leur réputation en ligne. D'autre part, ils n'exercent guère de contrôle sur ce que les autres peuvent publier à leur sujet et sur la façon dont les personnes et les organisations pourraient interpréter leurs renseignements personnels dans d'autres contextes, sur la période de conservation de ces renseignements ou sur l'incidence qu'ils auront sur leur réputation.

En 2016-2017, dans le cadre de ses efforts pour faire progresser l'une de ses priorités stratégiques en matière de protection de la vie privée, soit la réputation et le respect de la vie privée, le Commissariat a mené une consultation et lancé une demande d'articles sur la réputation en ligne. Cette consultation était articulée autour d'un document de travail sur la réputation et la vie privée préparé par le Commissariat et publié en janvier 2016. Nous avons demandé aux participants à la consultation de trouver des façons nouvelles et novatrices de protéger la vie privée et la réputation. Notre consultation visait à enrichir le débat public et à faire en sorte que le Commissariat soit bien placé pour proposer au Parlement diverses solutions afin de régler les problèmes liés à la réputation en ligne.

Bon nombre des mémoires reçus dans le cadre de la consultation comprenaient des observations sur le « droit à l'oubli »—en fait, de nombreux mémoires traitaient exclusivement de ce sujet. Selon la définition retenue par la Cour de justice de l'Union européenne, il s'agit du droit des individus de demander que certains liens soient retirés des résultats des moteurs de recherche, si ces liens renvoient à des renseignements inexacts, non pertinents ou périmés, sauf si ce sont des renseignements d'intérêt public.

Tout en reconnaissant les préjudices qui peuvent découler d'un « Internet qui n'oublie jamais », les auteurs de certains mémoires ont soulevé de sérieuses préoccupations quant à l'incidence qu'aurait la reconnaissance officielle du droit à l'oubli sur la liberté d'expression. Les auteurs d'autres mémoires se demandaient si la LPRPDE s'applique même à plusieurs aspects de la réputation en ligne ou aux moteurs de recherche, lesquels constituent des acteurs de premier plan dans ce débat, réclamant plutôt d'autres solutions. Mentionnons une utilisation accrue de lois ciblées pour prévenir des préjudices particuliers, de meilleures activités de sensibilisation concernant l'utilisation sûre et appropriée d'Internet (particulièrement dans le cas des populations vulnérables) ainsi que des pratiques améliorées pour les sites Web et les services en ligne comme les réseaux sociaux.

À la lumière de nos propres recherches ainsi que des commentaires et des avis que nous avons reçus dans le cadre de nos consultations, nous nous sommes penchés sur des façons nouvelles et novatrices de protéger la vie privée et la réputation, notamment sur la question de savoir si le droit à l'oubli pouvait s'appliquer dans le contexte canadien. La LPRPDE prévoit plusieurs mesures de contrôle, entre autres la possibilité de retirer son consentement, de

contester l'exactitude de renseignements et d'obliger les organisations à conserver les renseignements seulement pendant la période strictement nécessaire pour la réalisation des fins déterminées. Il y a aussi d'autres mesures de contrôle découlant d'une source autre que la LPRPDE, notamment des délits récemment reconnus[7] comme la communication de faits confidentiels embarrassants, ainsi que des nouvelles lois fédérales contre la cyberintimidation et la pornographie vengeresse.

Nos enquêtes sur des questions connexes soulevées par des plaignants nous aident aussi à orienter nos réflexions sur la question de la réputation. Par exemple, le site Web roumain Globe24h.com, qui publiait les décisions de tribunaux du monde entier, y compris du Canada, a fait l'objet de nombreuses plaintes déposées auprès du Commissariat par des individus alléguant que Globe24h utilisait leurs renseignements personnels dans un but lucratif sans leur consentement. En 2015, nous avons publié les conclusions de notre enquête sur Globe24h notre site Web.

À la suite de la diffusion de notre rapport d'enquête, un plaignant a déposé une requête devant la Cour fédérale en réclamant des dommages-intérêts à Globe24h ainsi qu'une ordonnance exécutoire pour obliger l'exploitant du site à supprimer sur ses serveurs toutes les décisions de tribunaux canadiens. Comme il s'agissait d'enjeux susceptibles de créer un précédent, le Commissariat est intervenu dans le litige. En janvier 2017, la Cour fédérale a confirmé les conclusions de notre enquête et a ordonné à Globe24h de retirer du site Web les décisions judiciaires du Canada renfermant des renseignements personnels et de s'abstenir par la suite de copier et de republier les décisions canadiennes d'une manière qui contrevient à la LPRPDE. Le tribunal a également ordonné à l'organisation de verser des dommagesintérêts symboliques en raison de ses pratiques irrégulières.

La décision confirme l'application de la LPRPDE aux activités des organisations d'autres pays utilisant des renseignements personnels et ayant un lien réel et substantiel avec le Canada. Elle montre aussi comment la hausse de la circulation transfrontalière de renseignements a créé à l'échelle mondiale des risques d'atteinte à la vie privée qui requièrent une intervention internationale.

Le Commissariat élabore actuellement une position de principe sur la réputation en ligne qu'il présentera au Parlement avant la fin de 2017. En fin de compte, la LPRPDE était une loi efficace et, à certains égards, novatrice au moment de son entrée en vigueur en 2001 et elle continue d'offrir une assise solide sur laquelle on peut s'appuyer. Cependant, l'ampleur et le rythme des avancées technologiques et des innovations commerciales au cours des années qui ont suivi, tout en créant des possibilités remarquables, exercent une forte pression sur la capacité des individus à protéger leur vie privée. Afin de relever les défis en matière de protection de la vie privée dans un monde numérique et de répondre aux attentes des Canadiens à cet égard, la LPRPDE doit être modernisée.

7 Actes répréhensibles qui causent un préjudice à un individu, à ses biens, à sa réputation ou à d'autres éléments par suite desquels la partie lésée a droit à une indemnisation.

TRAVAUX PROACTIFS À L'APPUI DU RESPECT DE LA VIE PRIVÉE—AIDER LES CANADIENS À EXERCER LEURS DROITS ET SENSIBILISER LES ORGANISATIONS À LEURS OBLIGATIONS

La protection du droit à la vie privée des Canadiens doit nécessairement comprendre des efforts proactifs pour aider les Canadiens eux-mêmes à comprendre leurs droits et à les exercer ainsi que pour aider les organisations à comprendre les obligations qui leur incombent en matière de protection de la vie privée en vertu des lois fédérales.

Les enquêtes du Commissariat sur les plaintes ont suscité de nombreuses améliorations aux pratiques de protection de la vie privée des organisations, mais l'ère numérique s'accompagne de nouveaux défis que notre modèle axé sur les plaintes ne nous permet pas toujours de relever—les individus sont peu susceptibles de déposer une plainte à propos d'un fait dont ils ignorent l'existence. Et à l'ère des mégadonnées et de l'Internet des objets, on peut difficilement savoir et comprendre ce qu'il advient de nos renseignements personnels.

D'après notre plus récent sondage, 92 % des Canadiens étaient préoccupés par la protection de leur vie privée. Près de la moitié des répondants avaient l'impression de ne plus avoir de contrôle sur la façon dont les organisations recueillent et utilisent leurs données. Ces propos sont troublants. Certaines choses doivent changer, sans quoi les Canadiens pourront perdre confiance dans l'économie numérique, ce qui entraverait sa croissance et limiterait leur capacité de bénéficier de tous les avantages de l'innovation. Plus important encore, dans une société démocratique, il est très malsain que la plupart des citoyens craignent que l'un de leurs droits les plus fondamentaux ne soit pas respecté.

À l'avenir, nous mesurerons le succès de nos activités d'après la capacité d'action des citoyens. Si notre objectif est de réduire la proportion de Canadiens inquiets pour leur vie privée, nos activités doivent être considérées comme utiles pour les individus et les organisations. Elles doivent aussi inciter les organisations à se conformer aux lois canadiennes sur la protection des renseignements personnels.

Signalons que le Commissariat a expressément le mandat, en vertu de la LPRPDE, de mener ce type d'activités de communication et de sensibilisation et de faire des recherches sur des enjeux liés à la protection de la vie privée. Dans nos mémoires au Parlement concernant la modernisation de la *Loi sur la protection des renseignements personnels*, nous avons recommandé de la modifier de façon à conférer expressément au Commissariat un pouvoir similaire d'être plus proactif afin de sensibiliser le secteur public fédéral aux questions relatives à la vie privée.

Au cours du dernier exercice, le Commissariat a entrepris un large éventail de travaux proactifs afin d'aider, d'une part, les Canadiens à protéger leur vie privée et, d'autre part, les institutions et les organisations des secteurs public et privé à s'acquitter de leurs obligations relatives à la protection de la vie privée.

Information et éducation du public

Le Commissariat contribue à l'éducation et à la sensibilisation du public au sujet des droits et des enjeux liés à la vie privée en menant différentes activités de communication—allocutions et activités spéciales, mobilisation des Canadiens par les médias et diffusion de matériel promotionnel et éducatif par diverses méthodes.

Nouveau site Web du Commissariat

Le site Web du Commissariat compte plus de deux millions de consultations par année, ce qui en fait son principal outil pour communiquer avec les Canadiens. En septembre 2016, nous avons lancé une version remaniée du site Web pour le rendre plus centré sur les citoyens et mieux répondre aux besoins des nombreux utilisateurs. En plus d'améliorer la conception et d'ajouter des fonctions de navigation clés, nous avons réorganisé l'information par sujets afin que les utilisateurs puissent trouver plus facilement l'information dont ils ont besoin.

Nous avons aussi ajouté un nouvel outil de « rétroaction » que les visiteurs peuvent utiliser pour nous indiquer s'ils ont trouvé une orientation ou un conseil précis utile ou non, et préciser pourquoi, ce qui nous aidera à continuer d'améliorer le site.

Amélioration de l'information et des conseils pour les Canadiens

Dans le cadre de notre objectif consistant à simplifier le matériel d'éducation du public et à élaborer des conseils et des orientations concernant les sujets qui préoccupent les Canadiens, le Commissariat a mis à jour ou a préparé de l'information et des conseils sur divers enjeux clés, entre autres le droit à la vie privée dans les aéroports et aux postes frontaliers, les accessoires intelligents à porter sur soi, la protection de la vie privée en ligne, l'Internet des objets, l'accès aux renseignements personnels et les services de dépistage génétique offerts directement aux consommateurs. Nous révisons actuellement l'information sur ce dépistage à la lumière de l'adoption récente du projet de loi S-201, *Loi sur la non-discrimination génétique*, qui représente un progrès important pour les Canadiens et que nous avons appuyé devant le Parlement plus tôt cette année.

Dans l'avenir, le Commissariat continuera de cerner les principaux enjeux pour lesquels de l'information et des conseils pour les individus sont demandés ou justifiés, de mettre à jour ou d'élaborer ce contenu et de le promouvoir activement par les voies de communication et de sensibilisation tant traditionnelles que nouvelles et novatrices.

Communications et sensibilisation au sein des groupes vulnérables

Le Commissariat a aussi lancé des initiatives ciblées en matière de communications et de sensibilisation pour entrer en contact avec certains groupes vulnérables, plus particulièrement les personnes âgées et les jeunes, afin de les aider à mieux comprendre leur droit à la vie privée. Au cours de l'établissement des priorités, nous avons déterminé que ces groupes bénéficieraient le plus d'information et de soutien accrus en lien avec les questions relatives à la protection de la vie privée. Puisque les jeunes adoptent rapidement les nouvelles technologies et publient généralement beaucoup d'information sur eux-mêmes en ligne, nous estimons qu'ils sont exposés à des risques particulièrement élevés d'atteinte à leur réputation. Il en va de même pour les aînés en raison de leur vulnérabilité au vol d'identité et de leur manque d'expérience relatif en ce qui concerne les nouvelles technologies en ligne.

Au cours du dernier exercice, nous avons mené plusieurs initiatives de sensibilisation ciblant ces deux groupes. Notre campagne à l'intention des personnes âgées comprenait, par exemple, des illustrations et des messages figurant sur les relevés de prêts de bibliothèques partout au Canada; la production de messages radio portant sur des sujets de préoccupation pour les aînés, notamment le vol d'identité et la protection de la vie privée en ligne; et des publipostages électroniques par l'intermédiaire de partenaires comme l'Association canadienne des individus retraités (ACIR) et la Fédération de l'âge d'or du Québec (FADOQ).

Notre campagne auprès des jeunes comprenait des allocutions (par exemple, devant les membres de la Fédération canadienne des enseignantes et des enseignants), des stands d'exposition dans le cadre des salons pour parents et enfants et d'autres activités axées sur la famille un peu partout au Canada. Nous avons aussi lancé une nouvelle page Facebook où sont

affichés des renseignements et des conseils destinés aux parents et au grand public concernant la protection de la vie privée en ligne. De plus, nous avons collaboré avec nos partenaires provinciaux et territoriaux et avec HabiloMédias afin de créer des plans de cours qui seront mis en œuvre dans les écoles en 2017-2018. Ces plans de cours font la promotion des compétences énoncées dans le *Référentiel de formation des élèves à la protection des données personnelles*, publié en octobre 2016 au cours de la Conférence internationale des commissaires à la protection des données et de la vie privée au Maroc. Ce référentiel porte sur la nécessité et l'urgence d'enseigner aux enfants comment protéger leurs données et leur vie privée dans le monde numérique d'aujourd'hui.

Le Commissariat mettra à jour ses stratégies de sensibilisation des aînés et des jeunes alors qu'il poursuivra ses efforts en vue de soutenir ces deux groupes, notamment ses démarches favorisant des activités d'éducation plus concrètes en ce qui a trait à la protection de la vie privée dans les programmes scolaires à l'échelle du Canada.

Renseigner les organisations sur leurs responsabilités en matière de protection des renseignements personnels

Comme nous l'avons déjà mentionné, la LPRPDE accorde au Commissariat le mandat de mener, entre autres, des activités d'éducation du public pour promouvoir la conformité à la Loi. L'une des façons d'y parvenir consiste à entreprendre des initiatives visant à renseigner les organisations sur leurs obligations en matière de protection des renseignements personnels.

Sensibilisation des petites entreprises

Selon un sondage mené par le Commissariat auprès des entreprises, celles de petite taille sont moins sensibilisées que les grandes organisations à leurs responsabilités en matière de protection des renseignements personnels. En outre, moins il y a d'employés, plus le niveau de connaissance dans le domaine est faible au sein d'une organisation. Nous avons déployé une stratégie pluriannuelle pour aider les petites entreprises à mieux comprendre leurs responsabilités en matière de protection des renseignements personnels et à se conformer à la législation dans le domaine. Cette stratégie repose sur une approche sectorielle et globale.

En mars 2017, nous avons terminé la première phase de la stratégie. Sur une période de 18 mois, nous avons mis l'accent sur la sensibilisation des secteurs de l'hébergement locatif et du commerce de détail—les deux secteurs où le nombre de plaintes déposées contre des petites entreprises concernant la protection des renseignements personnels était le plus élevé. Nous avons rencontré des associations d'industrie, participé à des discussions et à des expositions pour joindre ces groupes, formulé des conseils propres à ces secteurs pour surmonter les difficultés en matière de protection des renseignements personnels et diffusé des messages par d'autres voies de communication directes, comme leurs bulletins électroniques.

Nous avons aussi mené des activités pour joindre l'ensemble des petites entreprises. Par exemple, nous avons donné des présentations devant des petites entreprises et tenu des stands d'exposition dans le cadre d'activités organisées dans différentes villes à la grandeur du Canada en collaboration avec les chambres de commerce, Facebook et d'autres associations d'industrie à l'intention de secteurs clés; joint un encart à un envoi postal de l'Agence du revenu du Canada adressé à plus de 500 000 petites entreprises; et diffusé des conseils et des orientations sur la protection des renseignements personnels via les chaînes d'affaires populaires d'Innovation, Sciences et Développement économique Canada sur Facebook et Twitter.

Dans l'avenir, nous avons l'intention de continuer à essayer de renseigner les petites entreprises sur leurs responsabilités en matière de protection des renseignements personnels. Nous redoublerons d'efforts au cours des prochains mois pour sensibiliser

davantage de nouveaux secteurs, particulièrement les entreprises en ligne et en démarrage ainsi que les professionnels du droit.

Orientations à l'intention des organisations

En plus de déployer des efforts auprès des petites entreprises, le Commissariat mène plusieurs activités pour aider les organisations en général à comprendre leurs responsabilités en matière de protection des renseignements personnels. Ces activités de sensibilisation et les relations avec les intervenants peuvent s'avérer une façon rentable de promouvoir la conformité proactive à la LPRPDE. Ces types d'activités offrent également au Commissariat une perspective précieuse et des renseignements commerciaux utiles concernant les questions de protection des renseignements personnels, les pratiques de l'industrie, les préoccupations des consommateurs ainsi que les tendances, les possibilités et les défis nouveaux.

Mentionnons notamment la publication régulière du résumé de conclusions d'enquêtes visant les entreprises, qui donnent des exemples concrets de la façon dont la LPRPDE s'applique dans la gestion quotidienne des renseignements personnels au sein des entreprises. Nous avons présenté 28 cas sur notre site Web au cours du dernier exercice.

En 2016-2017, le Commissariat a aussi mis à jour l'information existante et donné de nouvelles orientations à l'intention des entreprises dans plusieurs domaines différents, notamment de l'information sur l'application d'articles particuliers de la LPRPDE et le furetage par les employés. Notre enquête sur l'atteinte massive à la sécurité des données sur le site de rencontres en ligne Ashley Madison a aussi permis de dégager des leçons que les entreprises pourraient mettre à profit pour améliorer leurs pratiques de protection des renseignements personnels.

De plus, à la suite du dépôt du projet de loi S-4, *Loi sur la protection des renseignements personnels numériques*, la LPRPDE a été modifiée en 2015 pour permettre aux organisations, dans certaines circonstances, de communiquer des renseignements personnels à une autre organisation à l'insu de l'intéressé et sans son consentement dans certains cas liés à des enquêtes ou à des fraudes. Les entreprises ont consulté le Commissariat pour obtenir des orientations concernant l'incidence de la nouvelle loi sur leurs obligations en matière de protection des renseignements personnels. Nous avons publié des orientations sur ces dispositions et rappelé aux organisations que ces exceptions acceptables dans certaines circonstances ne permettent pas de communiquer des renseignements personnels de façon arbitraire.

Le Commissariat a également mis en œuvre une nouvelle initiative de séances d'analyse. Ces activités, sous forme d'ateliers, fournissent aux intervenants de l'information à jour et une perspective approfondie sur des conclusions d'enquête dans des cas importants et leur offrent la possibilité de prendre part à des discussions et de poser des questions. Nous avons tenu deux séances d'analyse au cours du dernier exercice, soit une sur le dossier Ashley Madison et l'autre sur l'enquête visant Compu-Finder menée par le Commissariat en vertu de la Loi canadienne anti-pourriel. Les deux séances ont attiré de nombreux participants et nous prévoyons en tenir davantage dans l'avenir.

Le commissaire et d'autres représentants du Commissariat ont aussi donné des présentations dans le cadre de différentes conférences et activités d'apprentissage à l'intention des fonctionnaires fédéraux sur des questions concernant la protection de la vie privée, notamment au cours d'une réunion du milieu de l'accès à l'information et de la protection des renseignements personnels en avril 2016 et d'une activité s'inscrivant dans le cadre de la Semaine de sensibilisation à la sécurité en février 2017. De plus, nous avons publié les *Conseils clés en matière de protection des renseignements personnels à l'intention des professionnels des ressources humaines du gouvernement fédéral* reposant

sur des exemples réels d'enquêtes menées par le Commissariat en vertu de la *Loi sur la protection des renseignements personnels*. Nous demeurons en contact avec le Secrétariat du Conseil du Trésor (SCT) en ce qui a trait à la protection de la vie privée au sein du gouvernement fédéral.

En outre, le Commissariat a lancé une série de blogues visant à démystifier les nouvelles technologies de l'information et à expliquer leur incidence sur la vie privée. À ce jour, nous avons diffusé de l'information portant, par exemple, sur les rançongiciels, les assistants virtuels, les réseaux privés virtuels et l'authentification.

Comparutions devant le Parlement en lien avec la LPRPDE

Le Commissariat rend compte au Parlement des questions qui ont une incidence sur le droit des Canadiens à la vie privée en comparaissant devant lui et en lui présentant des mémoires. En plus des comparutions et des mémoires dont fait état la section du présent rapport consacrée aux comparutions devant le Parlement en lien avec la *Loi sur la protection des renseignements personnels* (voir page 94), plusieurs comparutions et mémoires du Commissariat en 2016-2017 portaient expressément sur des questions relevant de la LPRPDE—certains sont présentés en détail dans d'autres sections du rapport. Dans l'ensemble, nous constatons un accroissement encourageant de l'attention portée par les parlementaires aux questions concernant la vie privée.

Au cours de l'exercice, le Commissariat a comparu devant le Parlement à 13 reprises et présenté 16 mémoires à des comités parlementaires. Outre nos comparutions et nos mémoires sur l'étude de la LPRPDE, la réforme de la *Loi sur la protection des renseignements personnels* et les questions de sécurité nationale, nous avons donné des avis au Parlement sur divers autres enjeux, dont la conduite avec facultés affaiblies et les véhicules connectés et autonomes.

Véhicules connectés

Le Commissariat a comparu devant le Comité sénatorial permanent des transports et des communications dans le cadre de son étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés. Les véhicules connectés et la protection de la vie privée ne sont pas foncièrement incompatibles, mais il y a des défis à relever. Grâce à l'intégration des mesures de protection appropriées, les Canadiens pourraient avoir l'assurance que leur vie privée sera protégée et par conséquent ils seraient plus à même de profiter des avantages des véhicules connectés et autonomes.

Comme il a été souligné dans la déclaration au Comité, les véhicules modernes sont plus qu'un simple moyen de transport—ils sont devenus des téléphones intelligents sur roues. Des capteurs recueillent de plus en plus de renseignements sur les systèmes du véhicule—des données à partir desquelles on peut extrapoler d'autres renseignements concernant le conducteur du véhicule, par exemple son mode de conduite ainsi que ses allées et venues. De plus, la sophistication et la connectivité croissantes des soi-disant « systèmes d'infodivertissement » permettent de recueillir des renseignements concernant la navigation, la circulation, la météo ou des divertissements, par exemple la diffusion audio en continu. Ces systèmes peuvent être jumelés avec le téléphone du conducteur pour permettre les communications mains libres, ce qui donne accès à sa liste de contacts de même qu'à ses appels entrants, à ses messages texte et à ses courriels.

Le Commissariat a exprimé son accord avec d'autres intervenants qui ont comparu devant le Comité en insistant sur l'importance de la protection de la vie privée dès la conception. Selon cette approche, les entreprises prennent en compte cette protection dès le départ et selon le point de vue de l'organisation dans son ensemble lorsqu'elles conçoivent de nouvelles technologies, par exemple un véhicule connecté. Aux États-Unis, par exemple, les constructeurs automobiles ont élaboré ensemble une série de principes de

protection des renseignements personnels similaires à ceux qui figurent dans la LPRPDE et ils se sont engagés à les respecter.

L'arrivée des véhicules connectés et autonomes peut présenter des avantages considérables pour les Canadiens. Mais ces technologies ne pourront obtenir la confiance des consommateurs que lorsqu'un juste équilibre sera atteint entre le flux d'information et la protection de la vie privée. Par ailleurs, dans le cadre de son Programme des contributions (voir ci-après), le Commissariat finance également un projet visant à élaborer un code de pratique pour les véhicules connectés.

Recherche

Programme des contributions

Le Commissariat finance la recherche indépendante et les initiatives connexes d'application des connaissances portant sur la protection de la vie privée par l'entremise de son Programme des contributions. Un montant de 500 000 $ par exercice est offert dans le cadre du programme.

Ce programme a pour but de générer de nouvelles idées, approches et connaissances sur la protection de la vie privée que les organisations pourront mettre en œuvre pour mieux protéger les renseignements personnels ou que les Canadiens pourront utiliser pour prendre des décisions plus éclairées en ce qui a trait à la protection de leur vie privée.

En 2016-2017, le Commissariat a lancé trois appels de propositions dans le cadre de son Programme des contributions et accordé un financement pour 14 projets de recherche et initiatives connexes d'application des connaissances portant notamment sur la vie privée des jeunes en ligne, les répercussions des services de généalogie sur la vie privée, les risques d'atteinte à la vie privée associés aux technologies intelligentes à porter sur soi et l'anonymisation des données.

Soulignons que le Commissariat a également financé au cours de l'exercice un troisième symposium de recherche Parcours de protection de la vie privée, organisé par l'Université de Toronto sur le thème « La protection de la vie privée en ligne : L'approche centrée sur la personne ». Les participants ont exploré les valeurs à la base de la protection de la vie privée en ligne et se sont efforcés de déterminer en quoi les avancées technologiques menacent ces valeurs.

ENQUÊTES EN VERTU DE LA LPRPDE

Le Commissariat mène des enquêtes indépendantes et impartiales sur les pratiques de traitement des renseignements personnels des entreprises assujetties à la LPRPDE.

Le nombre total de plaintes acceptées par le Commissariat est demeuré stable en 2016-2017, soit 325 plaintes, comparativement à 332 pour l'exercice précédent[8].

Comme au cours des exercices antérieurs, les secteurs des finances et de l'Internet ont continué à faire l'objet d'un nombre élevé de plaintes. Ensemble, ces secteurs représentaient plus du tiers (35 %) des plaintes acceptées. En ce qui a trait aux types de questions que nous examinons, plus de la moitié des dossiers clos au cours du dernier exercice concernaient des questions relatives au consentement (30 %) et l'accès aux renseignements personnels (30 %).

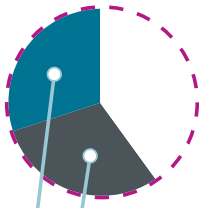
En 2016-2017, nous avons mené à bien 294 enquêtes, soit un nombre comparable aux 281 dossiers clos au cours de l'exercice précédent.

ENQUÊTES MENÉES EN 2016–2017 – LPRPDE

325 plaintes acceptées

Secteurs des **finances** et de **l'internet : 35 %** des **plaintes acceptées**

Plus de la moitié des **294 dossiers clos** au cours du dernier exercice portaient sur le **consentement** (30 %) et **l'accès** aux **renseignements personnels** (30 %)



8 L'« exercice précédent » correspond à la période de 12 mois commencée le 1er avril 2015 et terminée le 31 mars 2016. Les données statistiques sur les activités en vertu de la LPRPDE figurant dans le Rapport annuel au Parlement 2015–2016 concernant la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur la protection des renseignements personnels correspondent à une période de 15 mois, car le cycle de production des rapports est passé de l'année civile à l'exercice financier.

Règlement rapide

Nous avons poursuivi nos efforts afin de régler les plaintes par règlement rapide, ce qui constitue une méthode moins formelle, plus rapide et moins cher pour traiter des plaintes relativement simples. En 2016-2017, nous avons réussi à fermer de cette façon 70 % des dossiers, par rapport à 50 % lors de l'exercice précédent, ce qui nous a permis de ramener de sept mois en 2015-2016 à 5,1 mois en 2016-2017 le délai moyen de traitement des plaintes. Les dossiers réglés rapidement ont été fermés après 2,6 mois en moyenne, comparativement à 10,7 mois pour les plaintes nécessitant une enquête complète.

Étude de plaintes réglées rapidement

En plus d'être efficace, le règlement rapide peut mener à des changements d'une portée plus grande qui renforcent la protection de la vie privée. Le cas suivant montre comment le règlement rapide a amélioré les pratiques de protection des renseignements personnels.

Le Commissariat a reçu une plainte mettant en cause une entreprise de services en ligne qui permet aux utilisateurs d'avoir accès à leurs renseignements personnels détenus par d'autres organisations au moyen de leurs interfaces logicielles. Le plaignant alléguait que des renseignements personnels qui ne le concernaient pas s'affichaient en dépit des multiples demandes pour que l'entreprise corrige le problème. Nous avons communiqué avec l'entreprise et découvert que le problème était attribuable à une erreur technique impliquant l'interface logicielle d'une autre organisation. Nos discussions avec l'entreprise et l'autre organisation ont permis de corriger l'erreur au bénéfice de tous les utilisateurs et le problème du plaignant a été réglé à sa satisfaction.

À la suite de l'intervention du Commissariat, l'entreprise de services en ligne a :

- modifié ses politiques et ses procédures internes relatives au traitement des préoccupations concernant la protection des renseignements personnels soulevées par les clients à son Centre de service à la clientèle en intégrant un processus d'acheminement à son chef de la protection des renseignements personnels;
- collaboré avec l'autre organisation pour corriger l'erreur technique à l'origine de l'affichage accidentel de renseignements personnels concernant une mauvaise personne;
- conclu avec l'autre organisation un accord contractuel pluriannuel qui couvre tout problème technique susceptible de survenir dans la prestation des services, qui comprend des dispositions améliorées sur le consentement de l'utilisateur et qui accroît les avantages mutuels découlant de la conformité à la LPRPDE.

Refus d'enquêter ou abandon des enquêtes

En plus de profiter de la possibilité de clore davantage de dossiers par règlement rapide et de maximiser ainsi notre capacité et notre efficacité en matière d'enquêtes, nous avons exercé davantage les pouvoirs que nous confère la LPRPDE pour refuser ou abandonner les plaintes restantes. Ces pouvoirs s'appliquent, par exemple, si une personne ayant déposé une plainte au Commissariat a également porté l'affaire devant les tribunaux. Au cours de l'exercice, le Commissariat a plus que doublé le nombre de refus ou d'abandon d'enquêtes, lesquels représentent maintenant environ 40 % de ses enquêtes fermées autrement que par règlement rapide.

Optimisation des ressources

Malgré l'importance soutenue accordée à la résolution des plaintes par règlement rapide et une utilisation plus judicieuse du pouvoir de refuser ou d'abandonner des enquêtes, nous n'arrivons pas à répondre aux exigences associées aux plaintes complexes—des cas touchant un grand nombre d'individus ou reposant sur des allégations d'infractions à la Loi particulièrement flagrantes. Les technologies émergentes, les nouvelles pratiques commerciales et les nouveaux modèles d'affaires qui utilisent des renseignements personnels ajoutent à la complexité de ces plaintes, si bien qu'il est plus difficile de clore des enquêtes en respectant la norme de service de 12 mois prévue par la Loi.

Résumé des principales enquêtes

Comme au cours des exercices antérieurs, la question du consentement à la collecte, à l'utilisation et à la communication de renseignements personnels est demeurée en 2016-2017 un thème récurrent dans les plaintes faisant l'objet d'une enquête. Ainsi que le souligne notre rapport sur le sujet, le consentement devient de plus en plus complexe à l'ère numérique et il y a de nombreuses questions sur ce qui constitue des renseignements auxquels a accès le public et sur la façon dont on peut les utiliser. Voici quelques cas clés concernant le consentement qui ont fait l'objet d'enquêtes au cours de l'exercice.

Wajam Internet Technologies—Absence de consentement à l'installation d'un logiciel publicitaire

Comme la LPRPDE lui en confère le pouvoir, le commissaire à la protection de la vie privée du Canada a pris l'initiative d'une plainte contre Wajam Internet Technologies Inc. (Wajam) en juin 2016. Il s'agit de la seconde plainte traitée par le Commissariat en vertu de la *Loi canadienne antipourriel*.

L'entreprise canadienne a développé un logiciel appelé « Wajam » (renommé et commercialisé sous le nom de « Social2Search » par la suite). Une fois installé sur un ordinateur personnel, le logiciel suit les requêtes de recherche en ligne de l'utilisateur et ajoute l'information à d'autres résultats de recherche découlant de contenus partagés par les « amis » et les contacts de l'utilisateur dans les médias sociaux. Wajam affichait aussi des publicités d'après les recherches en ligne de l'individu. Le logiciel, installé principalement par l'intermédiaire de distributeurs tiers, serait ajouté à d'autres gratuiciels non reliés que les utilisateurs pouvaient télécharger.

Nos recherches ont révélé que plusieurs blogues de TI, articles et programmes antivirus classaient Wajam comme un publiciel ou un logiciel potentiellement indésirable. Nous avons également relevé des commentaires en ligne d'utilisateurs qui ne se rappelaient pas avoir consenti à l'installation du logiciel et d'autres indiquant qu'il était très difficile de le désinstaller.

La *Loi canadienne anti-pourriel* (LCAP) a modifié la LPRPDE pour limiter considérablement les cas où une organisation peut recueillir et utiliser des renseignements personnels sans consentement au moyen d'un logiciel qui a été installé sur l'ordinateur d'un individu. Notre enquête sur Wajam a mis en lumière l'importance pour les développeurs de logiciel d'obtenir le consentement valable et express à l'installation d'un logiciel donnant lieu à la collecte et à l'utilisation de renseignements personnels.

L'enquête visait à déterminer si l'entreprise obtenait un consentement valable des utilisateurs pour installer le logiciel, si elle les empêchait de retirer leur consentement en rendant difficile la désinstallation du logiciel et si elle protégeait adéquatement leurs renseignements personnels.

Notre enquête a permis de conclure que Wajam avait enfreint la LPRPDE relativement à chacun des points susmentionnés. Nous avons aussi déterminé que l'entreprise avait contrevenu à d'autres principes de la LPRPDE—absence d'un cadre de gestion de la protection des renseignements personnels (responsabilité), transparence insuffisante en ce qui a trait au fonctionnement du logiciel ainsi qu'à la collecte et à l'utilisation des renseignements personnels de l'utilisateur, et conservation des renseignements personnels des utilisateurs pour une durée indéterminée.

Nous avons formulé 12 recommandations pour amener l'entreprise à se conformer à la LPRPDE, notamment la mise en place d'un programme de gestion des renseignements personnels, une formation sur la protection de la vie privée à l'intention du personnel, des mesures améliorées pour assurer l'obtention du consentement avant l'installation, de l'information plus exacte sur le fonctionnement du logiciel et la façon dont les renseignements personnels des utilisateurs sont recueillis et utilisés, la suppression des renseignements personnels des utilisateur ayant désinstallé le logiciel, ainsi que le chiffrement de sa base de données principale.

Pendant notre enquête, l'entreprise a cessé de distribuer le logiciel au Canada. On nous a finalement informés que Wajam avait vendu ses actifs, y compris son logiciel, à Iron Mountain Technology Limited (« IMTL »), entreprise établie à Hong Kong qui n'avait pas l'intention de distribuer le logiciel au Canada.

Wajam a également affirmé avoir cessé de recueillir les renseignements personnels de Canadiens qui avaient déjà installé le logiciel et s'est engagée à détruire tous les renseignements personnels des utilisateurs encore en sa possession.

Pour en savoir plus, consultez la version intégrale du rapport sur les conclusions de notre enquête de Wajam.

Renseignements auxquels le public a accès
Collecte et utilisation de renseignements personnels pour des rapports sur l'historique de propriétés

Une personne s'était plainte qu'une entreprise spécialisée dans l'élaboration et la vente de rapports sur l'historique de propriétés recueillait, utilisait et communiquait des renseignements personnels sans avoir dûment obtenu le consentement des intéressés. Ces rapports comprenaient l'historique des ventes, indiquaient les réclamations d'assurance et précisaient, le cas échéant, si la propriété avait été utilisée pour la culture de marijuana ou la fabrication de méthamphétamines.

L'entreprise a cessé de donner l'historique des ventes dans ses rapports, mais elle a soutenu que les autres renseignements n'étaient pas assujettis aux dispositions sur le consentement de la LPRPDE. Selon elle, il ne s'agissait pas de renseignements personnels parce qu'ils concernaient une propriété et non un individu et que l'information relative à l'activité liée aux drogues était accessible au public.

L'entreprise a confirmé que ses rapports contiendraient uniquement de l'information sur les réclamations pour dommages à la structure ou à l'immeuble (p. ex. tempête, tremblement de terre ou inondation), lorsque le montant des réclamations n'était pas versé directement à l'individu. C'est en nous fondant sur cette information que nous avons convenu que les détails d'assurance ne constituaient pas des renseignements personnels.

Nous avons toutefois constaté que l'information sur l'activité liée aux drogues constitue des renseignements personnels, car cette information, seule ou combinée avec d'autres renseignements facilement accessibles, peut être associée à une personne identifiable—le propriétaire ou l'occupant de la propriété pendant les périodes visées—et révéler que cet individu a été impliqué dans une activité liée aux drogues. Nous avons aussi conclu qu'il ne s'agit pas de

renseignements « auxquels le public a accès » au sens de la Loi, du fait que les renseignements des services de police utilisés par l'entreprise pour fournir ses services ne répondent pas à la définition réglementaire précise et restreinte de « renseignements auxquels le public a accès » et ne peuvent donc pas être recueillis, utilisés ni communiqués sans consentement. L'entreprise a reconnu qu'elle n'avait pas essayé d'obtenir le consentement des individus puisqu'elle ne croyait pas que ces renseignements étaient des renseignements personnels.

L'entreprise, qui avait cessé de produire des rapports sur l'historique de propriétés en attendant la résolution de la plainte, a accepté de reprendre cette activité sans inclure de renseignements sur l'activité liée aux drogues.

Nous avons donc considéré que la plainte était fondée et résolue. Pour en savoir plus, consultez la version intégrale du rapport sur les conclusions de cette enquête.

Accords de conformité

La *Loi sur la protection des renseignements personnels numériques* (anciennement le projet de loi S-4) a reçu la sanction royale en juin 2015, donnant ainsi lieu à plusieurs modifications importantes à la LPRPDE. Mentionnons notamment une nouvelle disposition permettant au commissaire à la protection de la vie privée de conclure des accords de conformité avec les organisations du secteur privé. Ces accords peuvent être utilisés dans des situations où le commissaire a des motifs raisonnables de croire qu'une organisation a contrevenu ou est susceptible de contrevenir à la LPRPDE ou qu'elle n'a pas suivi une recommandation qui assurerait sa conformité à la Loi.

En vertu d'un accord de conformité, une organisation accepte de prendre certaines mesures pour se conformer à la LPRPDE; pour sa part, le commissaire à la protection de la vie privée accepte de ne pas intenter de poursuites judiciaires contre elle.

Le Commissariat a mis sur pied l'Unité de vérification de la conformité en juin 2016. Cette unité vérifie si les organisations respectent leur accord de conformité et assure la surveillance constante et la mise en œuvre en temps utile des recommandations découlant des plaintes jugées « fondées et conditionnellement résolues ». Dans le cadre de ce mandat, elle a géré la négociation de notre premier accord de conformité autonome, qui n'était lié à aucune enquête officielle découlant d'une plainte. Un accord autonome est un moyen efficace et rentable pour les organisations d'assurer le Commissariat que les mesures correctrices appropriées seront entièrement mises en œuvre, dans les situations où des enquêtes complètes exigeant beaucoup de ressources ne sont pas nécessaires pour exposer les faits pertinents.

Loi canadienne anti-pourriel

La *Loi canadienne anti-pourriel* (LCAP) est la loi fédérale régissant les pourriels et les autres menaces électroniques. Le Commissariat est chargé de l'application de cette loi conjointement avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence.

Les pourriels et les autres menaces électroniques transcendent les frontières et mettent souvent en cause des intervenants qui sont établis dans plus d'un pays ou qui en ciblent plusieurs. Afin de permettre une collaboration nationale et internationale dans ce type d'enquêtes, nous avons conclu deux protocoles d'entente : le premier nous permet d'échanger des renseignements et de collaborer dans des enquêtes avec nos partenaires chargés d'appliquer la LCAP, soit le CRTC et le Bureau de la concurrence, et le second, d'échanger des renseignements et de collaborer avec des organisations internationales ayant un mandat semblable au nôtre pour lutter contre les pourriels, les logiciels malveillants et les autres menaces électroniques en tant que membre du Unsolicited Communications Enforcement Network (UCENet).

L'enquête sur Wajam, telle que décrite à la page 53, représente notre deuxième enquête en lien avec la LCAP. Comme en fait état notre Rapport annuel 2015–2016, nous avons publié les conclusions de notre première enquête en application des dispositions de la LPRPDE régissant la « collecte d'adresses » (dans la foulée de la LCAP en juillet 2014). Après avoir échangé des renseignements avec le CRTC, le Commissariat a mené une enquête sur Compu-Finder, entreprise établie au Québec qui offre des cours de formation professionnelle. L'enquête a fait ressortir l'importance de collaborer avec nos partenaires chargés de l'application de la loi afin de conclure avec succès les enquêtes sur les pourriels.

Après avoir constaté que l'entreprise avait utilisé à des fins de marketing des adresses de courriel recueillies au moyen d'un logiciel de collecte d'adresses, nous avons conclu notre tout premier accord de conformité volontaire. Nous avons fait un suivi auprès de Compu-Finder en 2016-2017 sur le respect des modalités de l'accord et avons confirmé que Compu-Finder a mis en œuvre toutes les mesures requises par l'accord.

En appui à son travail lié à la LCAP, le Commissariat collabore aussi avec des organisations internationales analogues, sous l'égide de l'UCENet, et avec ses partenaires de l'industrie au sein du Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). Notre participation dans ces réseaux nous aide à accroître et à partager nos connaissances concernant les menaces en ligne ainsi que les tendances à cet égard et les méthodes pour les contrer. Par ailleurs, nous avons participé en 2017 au premier « ratissage » réglementaire de l'UCENet. Dans le cadre de cette initiative de collecte de renseignements, diverses autorités mènent des recherches coordonnées sur un thème précis. Le CRTC et le bureau du commissaire à l'information du Royaume-Uni pilotent la démarche, qui s'inspire du ratissage pour la protection de la vie privée du Global Privacy Enforcement Network (idée conçue et développée à l'origine par le Commissariat).

Atteintes à la vie privée

Comme au cours des exercices antérieurs, nous avons continué de recevoir un grand nombre de déclarations d'atteintes à la vie privée en vertu de la LPRPDE—près de 100 au cours de chacun des deux derniers exercices. Nous nous attendons à une augmentation appréciable du nombre de déclarations lorsque le règlement sur la déclaration obligatoire des atteintes à la vie privée entrera en vigueur.

Piratage du site Ashley Madison

En août 2016, le Commissariat a diffusé un communiqué résumant les conclusions d'une enquête sur une atteinte à la vie privée de grande ampleur en lien avec le site AshleyMadison.com. Ruby Corp. (anciennement « Avid Life Media », ou ALM) exploite ce site Web s'adressant aux personnes en quête d'aventures en toute discrétion. L'enquête a été menée en collaboration avec le Commissariat à l'information et à la protection de la vie privée d'Australie et la Federal Trade Commission des États-Unis, qui a publié ses conclusions plus tard au cours de l'année. Ce cas illustre la façon dont des organismes exerçant leurs activités à l'antipode l'un de l'autre peuvent collaborer pleinement pour appliquer leur loi respective sur la protection des renseignements personnels.

Notre enquête a révélé que les mesures mises en place par ALM pour protéger les renseignements personnels sensibles étaient inadéquates. Plusieurs éléments clés étaient absents du cadre de sécurité de l'entreprise, par exemple des politiques ou des pratiques de sécurité de l'information documentées et une formation adéquate des membres du personnel sur les obligations leur incombant en matière de sécurité et de protection de la vie privée. Ce cas a aussi mis au jour des problèmes au point de convergence des lois sur la protection des renseignements personnels et la protection des consommateurs : tromperie et consentement. Nous avons constaté au cours de notre enquête que l'entreprise faisait sa promotion en garantissant l'entière discrétion du service, mais qu'elle étayait

cette affirmation en affichant sur sa page d'accueil une icône mentionnant que le site était sécurisé et digne de confiance. De l'aveu des représentants de l'entreprise, cette icône avait été fabriquée de toutes pièces. Les enquêteurs ont conclu que l'utilisation d'une marque de confiance fictive signifiait que l'entreprise n'avait pas obtenu de consentement des individus de façon appropriée.

Nous continuons d'exercer une surveillance étroite pour déterminer si Ruby Corp. met en œuvre les mesures correctives qu'elle s'est engagée à prendre dans le cadre d'un accord de conformité. D'après les conclusions importantes concernant les mesures de protection et d'autres exigences de cette enquête, nous avons publié les leçons à tirer pour toutes les organisations. De plus, une séance d'information technique tenue par le Commissariat consacrée aux conclusions de cette enquête a suscité un vif intérêt auprès des organisations assujetties à la LPRPDE.

Agence mondiale antidopage

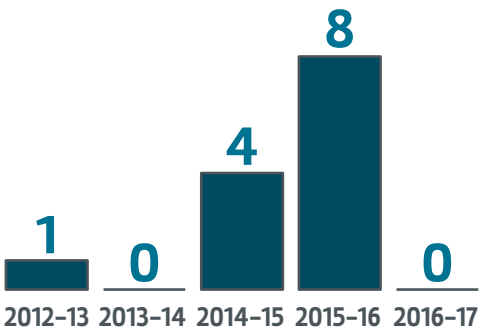
L'Agence mondiale antidopage (AMA) est notamment chargée de surveiller la conformité à la réglementation antidopage dans les sports. Cette organisation établie à Montréal a confirmé en septembre 2016 que sa base de données avait fait l'objet d'un accès inapproprié et que la confidentialité des données sur les athlètes était menacée. Les renseignements en question comprenaient des données médicales confidentielles comme les autorisations d'usage à des fins thérapeutiques permettant aux athlètes de prendre des médicaments qui seraient autrement considérés comme interdits afin de traiter une maladie ou une blessure.

Étant donné la sensibilité des renseignements, la nature de l'atteinte et les répercussions potentielles sur la vie privée et la carrière des athlètes canadiens et étrangers, le commissaire à la protection de la vie privée a exercé le pouvoir que lui confère la LPRPDE de prendre l'initiative de mener une enquête en novembre 2016. Cette enquête est en cours.

Communications à l'insu de l'intéressé ou sans son consentement—Avis envoyés par des organisations concernant le refus de communiquer des renseignements aux demandeurs

De façon générale, les individus peuvent présenter aux organisations une demande d'accès à l'information concernant les communications faites à des institutions fédérales en application de la LPRPDE. Cependant, dans certains cas, une organisation doit consulter les institutions fédérales compétentes pour déterminer si elle peut communiquer cette information au demandeur. L'institution fédérale peut s'opposer à la communication des renseignements pour les motifs énoncés au paragraphe 9(2.3) de la Loi, comme la sécurité nationale, le recyclage des produits de la criminalité ou l'application de lois. En pareil cas, l'organisation doit refuser de communiquer les renseignements et elle ne peut divulguer le fait que l'institution fédérale a été avisée. L'organisation doit aussi aviser le Commissariat du refus sans tarder.

Au cours des cinq derniers exercices, le Commissariat a reçu 13 avis de cette nature, soit dix émanant du secteur financier (banques et coopératives de crédit) et trois du secteur des télécommunications. Le Commissariat a publié un résumé de conclusions d'enquête qui donne des orientations aux organisations sur la façon de répondre aux demandes de communication de renseignements personnels à d'autres parties, notamment des organismes d'application de la loi.



NOMBRE D'AVIS ENVOYÉS EN VERTU DU PARAGRAPHE 9(2.4)

DOSSIERS RELATIFS À LA LPRPDE DEVANT LES TRIBUNAUX

Dans le cadre de la surveillance de la conformité à la LPRPDE, le Commissariat participe parfois à des procédures judiciaires en qualité de partie, de partie jointe ou d'intervenant pour faire respecter la Loi ou aider les tribunaux en faisant avancer l'interprétation et l'application de la loi.

Résumé des principaux dossiers

Banque Royale du Canada c. Trang, 2016 CSC 50

Le consentement éclairé et explicite de l'intéressé est exigé pour la collecte, l'utilisation ou la communication de renseignements personnels, mais il y a des exceptions—par exemple lorsque c'est nécessaire pour se conformer à une ordonnance d'un tribunal ou si l'on juge qu'une personne a donné son consentement implicite. Dans cette affaire, la Cour suprême du Canada (CSC) a donné de nouvelles orientations importantes sur l'application du consentement implicite.

Ayant obtenu un jugement du tribunal contre deux débiteurs, la Banque Royale du Canada (RBC) a voulu l'exécuter en vendant une propriété appartenant à ces derniers afin de régler leurs dettes. Toutefois, avant de procéder à la vente, elle devait obtenir l'état de mainlevée de l'hypothèque d'une autre banque pour montrer le statut de l'hypothèque à ce moment-là.

Comme il était impossible de trouver les propriétaires, la RBC a déposé une requête en vue d'obtenir une ordonnance obligeant le créancier hypothécaire à produire l'état de mainlevée en question. Le juge de première instance a affirmé que la LPRPDE lui interdisait de rendre l'ordonnance demandée.

La RBC a porté la décision en appel et invoqué plusieurs arguments, faisant valoir entre autres que les débiteurs avaient consenti implicitement à la communication des documents dans ce type de circonstances.

Dans une décision majoritaire, les juges de la Cour d'appel de l'Ontario ont donné tort à la RBC, déclarant qu'il n'y avait eu aucun consentement implicite dans les faits. Selon eux, la RBC pouvait obtenir une ordonnance du tribunal obligeant le créancier hypothécaire à produire l'état de mainlevée, mais la requête présentée devant le tribunal n'était pas admissible.

La RBC a été autorisée à interjeter appel devant la CSC. Même s'il n'était pas partie à la procédure, le Commissariat a participé en qualité d'« ami de la cour » devant la Cour d'appel de l'Ontario et la CSC.

La CSC a invalidé la décision de la Cour d'appel de l'Ontario en concluant que la requête présentée à l'origine par la RBC était suffisante pour rendre une ordonnance obligeant le créancier hypothécaire à produire le document. La CSC a aussi statué que le créancier hypothécaire pouvait s'appuyer sur le consentement implicite des débiteurs à la communication de l'état de mainlevée de l'hypothèque à la RBC.

Tout en confirmant que le consentement éclairé est un concept fondamental de la LPRPDE et qu'un consentement explicite s'impose de façon générale, la CSC a aussi confirmé que le consentement d'un individu peut être implicite—mais uniquement dans des circonstances strictement définies. Pour déterminer si un consentement implicite est approprié, une organisation doit évaluer en fonction du contexte la sensibilité des renseignements et les attentes raisonnables de l'individu. Dans cette évaluation, l'accès du public aux renseignements connexes ainsi que les intérêts et l'identité de l'organisation demandant la communication des renseignements pourraient être des facteurs pertinents.

Bertucci c. Banque Royale du Canada, 2016 CF 332

Dans une autre affaire, la Banque Royale du Canada (RBC) a fermé des comptes au nom de deux personnes, mais a refusé de leur communiquer l'information sur laquelle reposait cette décision. Les titulaires des comptes ont déposé une plainte auprès du Commissariat en alléguant que la banque leur refusait l'accès à leurs renseignements personnels. Le Commissariat s'est prononcé en faveur de la RBC au motif que la communication de l'information révélerait des renseignements commerciaux confidentiels—exception autorisée en vertu de la LPRPDE.

Les plaignants ont porté la cause devant la Cour fédérale, laquelle a conclu qu'une grande partie des renseignements conservés par la RBC n'étaient pas des renseignements commerciaux confidentiels, mais plutôt des « données brutes »—par exemple un article de journal sur les individus—et que la banque aurait dû leur donner accès aux données brutes en censurant les renseignements exclusifs au lieu d'opposer un refus général. La cour a souligné que le refus de communiquer des renseignements en vertu de l'article pertinent de la LPRPDE est assujetti à une norme « très rigoureuse »—l'accès aux renseignements personnels est la règle, alors que le refus de communiquer ces renseignements constitue l'exception.

Loi sur la protection des renseignements personnels

Rétrospective de l'exercice

RÉFORME DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Comme nous l'avons mentionné dans notre Rapport annuel 2015-2016, la *Loi sur la protection des renseignements personnels*, qui s'applique au secteur public fédéral au Canada, est demeurée pratiquement inchangée depuis sa promulgation en 1983. À l'époque, l'ordinateur personnel en était à ses balbutiements, le World Wide Web n'existait pas et le concepteur de Facebook n'était pas encore né.

Il n'y a aucun doute que l'évolution rapide et constante des technologies numériques continue d'offrir de nombreux avantages, comme l'amélioration de la prestation des services et un processus décisionnel plus efficace, mais ces technologies ont des répercussions profondes sur la vie privée et créent ainsi des risques que l'on n'aurait pu imaginer au moment de la rédaction de la *Loi sur la protection des renseignements personnels*. Les protections législatives, autrefois considérées comme révolutionnaires, remontent maintenant à plus de 30 ans, et elles ne sont tout simplement pas suffisantes pour protéger les renseignements personnels des Canadiens dans ce nouvel environnement. Par conséquent, on risque d'observer une collecte et à une communication excessives des renseignements personnels par les administrations publiques, à des atteintes à la vie privée de grande ampleur ainsi qu'à une érosion de la confiance des consommateurs dans l'économie numérique et envers nos institutions fédérales.

Le Parlement prend les premières mesures en vue de la modernisation

Le Commissariat à la protection de la vie privée du Canada demande depuis longtemps au gouvernement de moderniser la loi fédérale sur la protection des renseignements personnels dans le secteur public au Canada. Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes a annoncé en mars 2016 qu'il étudierait la *Loi sur la protection des renseignements personnels,* et le Commissariat a participé avec enthousiasme à cette étude.

Dans ses déclarations et ses mémoires à l'intention du Comité, le commissaire s'est efforcé de souligner l'importance d'une réforme législative et a proposé une série de modifications visant à contrer les nouvelles menaces pour la vie privée. En décembre 2016, après avoir entendu le témoignage

d'environ 45 intervenants, le Comité a publié son rapport final intitulé Protéger la vie privée des Canadiens : Examen de la *Loi sur la protection des renseignements personnels*. Nous étions heureux qu'il soit d'accord avec pratiquement toutes nos recommandations.

Nous étions également heureux que la ministre de la Justice déclare en réponse au rapport que son gouvernement mènerait lui-même un examen approfondi dans le but de moderniser la *Loi sur la protection des renseignements personnels*. Le Commissariat est impatient de participer à cet examen qui devrait, d'après nous, commencer sans tarder. De cette façon, nous continuerons de concentrer nos efforts sur les 16 recommandations concernant les changements technologiques, la modernisation des normes juridiques et l'accroissement de la transparence que nous avons formulées au Comité de l'ETHI.

Une recommandation clé formulée par le Commissariat préconise une modification de l'article 4 de la *Loi sur la protection des renseignements personnels*, qui se lit comme suit : « Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités. » À ce jour, le Commissariat a interprété cet article comme signifiant que les renseignements recueillis doivent être nécessaires à l'exécution d'un programme ou d'une activité. Cette interprétation est conforme à la Directive sur les pratiques relatives à la protection de la vie privée du SCT, c'est-à-dire que les institutions gouvernementales doivent limiter la collecte de renseignements personnels à ceux qui sont manifestement nécessaires ou exigés.

Cependant, cette interprétation n'est pas toujours appliquée. En fait, la Cour fédérale a récemment rendu une décision contre un seuil de « nécessité » (voir page 96), décision qui fait actuellement l'objet d'un appel.

Par souci d'une plus grande clarté et d'une certitude accrue du résultat de l'application de la *Loi sur la protection des renseignements personnels*, nous avons recommandé de prévoir et de définir dans la Loi une exigence explicite de nécessité pour la collecte de renseignements personnels. Cette mesure permettrait d'harmoniser la Loi avec les autres lois sur la protection des renseignements personnels en vigueur au Canada et à l'étranger.

Dans la correspondance échangée sur le sujet avec le président du Conseil du Trésor et la ministre de la Justice, ceux-ci ont indiqué qu'ils tiendraient compte de cette recommandation dans le cadre de leur examen en cours de la *Loi sur la protection des renseignements personnels* et que, dans l'intervalle, ils aviseraient les institutions fédérales d'appliquer le concept de nécessité à la collecte de renseignements personnels.

La prévention étant essentielle pour protéger la vie privée, nous avons aussi recommandé que la *Loi sur la protection des renseignements personnels* oblige les institutions fédérales à réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) (voir page 89) pour les activités et programmes comportant des renseignements personnels qui ont été nouvellement établis ou qui ont subi des modifications substantielles. Les institutions devraient aussi être tenues par la loi de présenter ces évaluations au Commissariat pour lui permettre de formuler des commentaires et des recommandations fondées sur leur analyse des risques.

Nous avons constaté que le processus des EFVP est très utile pour cerner et atténuer les risques d'atteinte à la vie privée avant la mise en œuvre d'un projet—et les institutions nous l'ont confirmé. La politique préconise cette pratique, mais elle n'est pas respectée par tous. D'ailleurs, des institutions continuent de présenter des EFVP tout juste avant, voire après la mise en œuvre de programmes.

Dans le même ordre d'idées, nous recommandons d'obliger les institutions fédérales à consulter le Commissariat concernant les projets de lois et de règlements ayant des répercussions sur la vie privée avant leur dépôt.

SÉCURITÉ NATIONALE, SÉCURITÉ PUBLIQUE, POSTES FRONTALIERS ET PROTECTION DE LA VIE PRIVÉE

La surveillance du gouvernement a été retenue comme l'une des quatre priorités stratégiques en matière de protection de la vie privée sur laquelle nous allions concentrer nos efforts. Notre objectif dans le domaine est de contribuer à l'adoption et à la mise en œuvre de lois et d'autres mesures qui assureront manifestement la sécurité nationale et la protection de la vie privée.

Personne ne niera la nécessité de veiller à la sécurité de nos citoyens. Les Canadiens veulent être en sécurité et se sentir protégés, mais pas au détriment de leur vie privée. Ce qu'ils désirent, c'est une approche équilibrée, mesurée et proportionnée. De nos jours, il serait trop naïf de croire que seuls les « méchants » ont à s'inquiéter pour leurs renseignements ou que « si on n'a rien à cacher, on n'a rien à craindre ».

Dans le même ordre d'idées, tout le monde conviendra que les services de police et les organismes de sécurité nationale ont besoin d'outils adéquats afin de s'acquitter de leur rôle essentiel consistant à assurer la sécurité des Canadiens et que ces outils doivent être adaptés au monde numérique. Cependant, les pouvoirs dont ils disposent ont *déjà* été renforcés de façon appréciable, plus particulièrement avec l'adoption des projets de loi C-51 (*Loi antiterroriste de 2015*) et C-13 (*Loi sur la protection des Canadiens contre la cybercriminalité*).

Il faut également se rappeler que nous avons été trop souvent témoins au cours de notre histoire d'activités inappropriées et parfois illégales de la part de représentants de l'État portant atteinte aux droits de citoyens ordinaires qui n'étaient soupçonnés d'aucun crime ni d'aucune activité terroriste. À notre avis, ces incidents graves sont attribuables à des normes juridiques déficientes ne fixant pas de limites appropriées aux mesures gouvernementales. Nous devons tirer des leçons clés de l'histoire : affaire Maher Arar, révélations d'Edward Snowden sur la surveillance de masse et cas plus récents mettant en cause l'accès sans mandat et la collecte de métadonnées par le Centre de la sécurité des télécommunications, le Service canadien du renseignement de sécurité (SCRS) et des services de police au Québec. L'histoire nous rappelle que des mesures de sécurité claires s'imposent pour protéger nos droits et prévenir les abus, que les organismes de sécurité nationale doivent faire l'objet d'un contrôle efficace et que l'octroi de nouveaux pouvoirs à l'État doit être justifié par des données probantes.

Nous avons affirmé que nous miserions sur des avis pertinents en temps utile concernant les évaluations des facteurs sur la vie privée, les ententes de communication des renseignements et les règlements pour réduire les risques d'atteinte à la vie privée associés à la *Loi antiterroriste de 2015* récemment adoptée. En ce qui a trait aux dispositions du projet de loi C-13 sur l'accès sans mandat, nous avons dit que nous collaborerions avec d'autres et donnerions des orientations aux secteurs public et privé afin d'établir des normes pour les rapports de transparence et de reddition de comptes concernant les entreprises qui communiquent des renseignements personnels à des organismes d'application de la loi. Nous avons aussi fait savoir que nous examinerions la mise en œuvre de la législation sur la sécurité nationale, comme le projet de loi C-51, et ferions rapport à cet égard. Nous avons ajouté que, en vertu de nos pouvoirs d'enquête et d'examen, nous examinerions les pratiques de collecte, d'utilisation et de communication des institutions participant aux activités de surveillance afin de nous assurer qu'elles se conforment à la *Loi sur la protection des renseignements personnels*.

La présente section porte sur les travaux du Commissariat au cours de l'exercice écoulé dans les domaines de la sécurité nationale, de la sécurité publique et des questions concernant la protection de la vie privée aux postes frontaliers.

Réponse à la consultation du gouvernement sur le cadre de sécurité nationale du Canada

À l'automne 2016, le gouvernement fédéral a publié un Livre vert sur la sécurité nationale dans le but d'« engager une discussion et un débat au sujet du cadre de sécurité nationale du Canada ». Il y a laissé entendre que les pouvoirs actuels de l'État n'étaient peut-être plus suffisants pour nous protéger à l'ère numérique. Le document indiquait plusieurs domaines où les pouvoirs des organismes de sécurité et d'application de la loi pourraient être accrus, ce qui faciliterait leur tâche dans bien des cas pour recueillir et échanger les renseignements personnels de Canadiens.

En décembre 2016, en partenariat avec les organismes provinciaux et territoriaux ayant un mandat similaire au sien, le Commissariat a déposé un mémoire officiel en réponse au *Livre vert sur la sécurité nationale*, afin d'attirer l'attention sur les risques d'atteinte à la vie privée associés à plusieurs propositions présentées dans le document. En plus de déposer ce mémoire, il a tenu une conférence de presse à l'Amphithéâtre national de la presse en face de la Colline du Parlement. Accompagné de Brian Beamish, commissaire à l'information et à la protection de la vie privée de l'Ontario, et de Jean Chartier, président de la Commission d'accès à l'information du Québec, le commissaire a présenté les points de vue et les recommandations du Commissariat.

Nous avons dit que le gouvernement devrait proposer un renforcement des pouvoirs de l'État et le Parlement devrait l'approuver uniquement s'ils sont manifestement nécessaires et proportionnés—et non simplement pratiques.

Dans son mémoire, le Commissariat a souligné la nécessité de gérer les risques d'atteinte à la vie privée liés à la communication d'information et à la collecte de métadonnées. Il a aussi soulevé des préoccupations à l'égard des propositions du gouvernement concernant l'accès des forces policières au contenu de base des abonnés détenues par les fournisseurs de services Internet et à leurs communications chiffrées.

Métadonnées

Tout en reconnaissant de façon générale que les enquêteurs des organismes d'application de la loi et de sécurité nationale doivent être en mesure de travailler efficacement autant dans le monde numérique que dans le monde réel, nous contestons dans notre mémoire l'idée qu'il faut abaisser les seuils prévus par la loi et réduire les mesures de protection connexes. Au contraire, on doit maintenir, voire renforcer les mesures de protection qui font depuis longtemps partie de nos traditions juridiques. Il faudrait aussi les adapter aux réalités des outils de communication modernes, qui permettent de conserver et de transmettre de grandes quantités de renseignements personnels extrêmement sensibles.

À notre avis, il est important de maintenir le rôle des juges dans la délivrance des mandats pour la collecte de métadonnées par les organismes d'application de la loi. Le maintien d'un rôle judiciaire est essentiel parce que les juges bénéficient de l'indépendance nécessaire pour assurer la protection des droits de la personne.

Le projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*, a déjà abaissé les seuils prévus par la loi pour l'accès aux métadonnées. En vertu de cette loi, il est possible d'obtenir auprès d'un juge une ordonnance de communication pour certains types de métadonnées s'il existe des « motifs raisonnables de soupçonner » qu'une infraction a été ou sera commise. Pourtant, les organismes d'application de la loi souhaiteraient que l'on abaisse encore les normes existantes. Les policiers ont-ils vraiment besoin d'avoir accès aux métadonnées s'ils n'ont même pas un soupçon raisonnable?

Nous ne comprenons pas pourquoi ces seuils si bas n'offrent pas aux organismes d'application de la loi des outils adéquats pour faire leur travail. Des cas récents de collecte de métadonnées montrent qu'il faudrait, en fait, rehausser les normes existantes et renforcer les mesures de protection de la vie privée.

Le Livre vert traite aussi d'enjeux se rapportant aux métadonnées dans le contexte de la sécurité nationale, mais il ne reflète pas à notre avis le fait que les métadonnées, loin d'être inoffensives, peuvent en révéler beaucoup plus sur les gens que le contenu réel des communications.

Le gouvernement affirme que les métadonnées sont essentielles pour mettre au jour les menaces, mais nous avons mentionné que des cas récents montrent que les activités du Centre de la sécurité des télécommunications (CST) et du Service canadien du renseignement de sécurité concernant les métadonnées peuvent porter atteinte à la vie privée de nombreux Canadiens qui ne mettent pas en péril la sécurité nationale. Le commissaire a indiqué qu'il faudrait renforcer les mesures de protection prévues par la loi pour régir ces activités.

Chiffrement

Le Livre vert du gouvernement a souligné que le chiffrement peut nuire aux enquêtes légitimes et à l'application des ordonnances judiciaires.

Cependant, le document accorde peu de poids au fait que le chiffrement constitue un outil essentiel pour la protection des renseignements personnels et la sécurité des appareils électroniques comme les téléphones intelligents. Il n'existe aucun moyen manifeste de donner un accès systémique au gouvernement sans exposer par le fait même la population générale à un risque élevé. Dans notre mémoire, nous avons exhorté le Parlement à faire preuve de prudence avant de prévoir des solutions par voie législative dans ce domaine complexe.

Le gouvernement a adopté des règles afin d'aider les organismes d'application de la loi à aborder la question du chiffrement. Par exemple, le projet de loi C-13 renferme une nouvelle disposition qui habilite les juges à annexer une ordonnance d'assistance à un mandat de perquisition ou à toute forme de surveillance électronique. L'ordonnance, qui oblige les personnes visées, y compris un suspect, à « prêter leur assistance » à l'exécution des actes autorisés, a été utilisée dans le cadre d'enquêtes pour passer outre à des dispositifs de sécurité ou obtenir des clés de déchiffrement.

Compte tenu de l'expérience et des facteurs observés, le commissaire a indiqué qu'il serait préférable d'explorer le domaine des solutions techniques—susceptibles de permettre un accès discret autorisé par la loi à des appareils chiffrés précis—au lieu d'imposer de nouvelles exigences par voie législative.

Communication d'information

Dans son mémoire, le Commissariat a signalé que le projet de loi C-51 présente des risques d'atteinte à la vie privée des Canadiens ordinaires en raison de l'accroissement considérable de l'ampleur et de la portée de la communication d'information par le gouvernement—problème exacerbé du fait que les mesures de protection de la vie privée laissent grandement à désirer.

Nous avons demandé au gouvernement d'envisager des modifications au projet de loi C-51, plus précisément en ce qui a trait aux dispositions autorisant la communication de renseignements personnels qui seraient simplement « pertinents » pour détecter de nouvelles menaces pour la sécurité. Nous avons souligné qu'une norme si faible explique en grande partie pourquoi les citoyens respectueux des lois sont exposés à des risques excessifs. Si, comme le prévoit la Loi sur le SCRS, le critère de la mesure « strictement nécessaire » est adéquat pour permettre au SCRS de recueillir, d'analyser et de conserver des informations, il est difficile d'expliquer pourquoi ce critère ne peut être adopté pour toutes les institutions qui jouent un rôle dans la sécurité nationale.

Dans le mémoire, nous avons fait valoir que le gouvernement n'avait pas clairement justifié la nécessité des nouvelles dispositions concernant la communication d'information. Nous y avons réclamé l'établissement de limites clairement définies quant à la période de conservation de l'information, l'obligation de conclure des ententes de communication d'information écrites et l'obligation, prévue par la loi, d'effectuer une EFVP pour évaluer et

atténuer les risques d'atteinte à la vie privée dans tous les programmes de sécurité nationale.

Nous avons également fait valoir dans le mémoire que les dispositions sur la communication d'information prévues dans le projet de loi C-51 ne sont pas le seul mécanisme donnant lieu à la communication d'information à des fins de sécurité nationale. Les mesures de protection comme la nécessité et la proportionnalité devraient s'appliquer à toute communication d'information à l'échelle nationale.

D'après le commissaire, il est également important que le Parlement tire des leçons de l'enquête sur Maher Arar et qu'il prenne des mesures pour réduire le risque que la communication d'information à des partenaires internationaux entraîne de graves violations des droits de la personne ainsi que des violations des obligations internationales du Canada.

Surveillance

Le commissaire a affirmé voir d'un bon œil l'intention du gouvernement de créer un nouveau Comité des parlementaires sur la sécurité nationale et le renseignement. Cette mesure constituera un pas en avant vers l'obligation démocratique de rendre des comptes. Il estime toutefois qu'un examen par des experts ayant une connaissance approfondie des activités menées par les organismes de sécurité nationale et des lois pertinentes s'impose aussi afin d'assurer une protection efficace des droits.

Il a également signalé que de nombreuses institutions ayant des obligations en matière de sécurité nationale, y compris l'Agence des services frontaliers du Canada et le Bureau du Conseil privé, ne font actuellement l'objet d'aucun examen particulier mené par des experts. Pour conclure, nous avons déclaré que ce n'est pas le moment de renforcer les pouvoirs de l'État et de réduire les droits individuels. Il est plutôt temps de renforcer les normes juridiques et la surveillance, de manière à ne pas répéter les erreurs du passé, et de trouver un juste équilibre entre la sécurité et le respect des droits individuels fondamentaux.

En juin, le gouvernement a déposé le projet de loi C-59. Entre autres, ce projet de loi sur la sécurité nationale prévoit la mise sur pied d'un Office de surveillance des activités en matière de sécurité nationale et de renseignement, chargé de surveiller ces activités à l'échelle du Canada et de faire enquête sur les plaintes se rapportant au SCRS, au CST et à la GRC. Le projet de loi vise aussi à créer le poste de commissaire au renseignement. Nous prévoyons faire part de notre point de vue sur ce projet de loi au Parlement en temps utile.

Vérifications et examens ayant trait à la sécurité nationale

Examen de la mise en œuvre et du mode d'application de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*

La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), déposée en janvier 2015 dans le cadre du projet de loi C-51, vise à encourager et à faciliter la communication d'information entre les institutions fédérales à des fins de sécurité nationale.

En 2016-2017, nous avons entrepris la deuxième phase de notre examen de la mise en œuvre et du mode d'application de la LCISC. Alors que la première phase était surtout axée sur l'ampleur des activités de communication d'information en vertu de la Loi, la deuxième portait principalement sur la nature des échanges d'information et les mécanismes en place pour s'assurer que les renseignements personnels sont traités conformément aux exigences des lois et des politiques.

Au cours de l'examen, nous avons constaté de graves lacunes dans les procédures de mise en œuvre et d'application de la LCISC, particulièrement l'absence de systèmes ou de processus pour surveiller et consigner l'information communiquée en vertu de la Loi. Les pratiques de tenue de documents variaient d'une institution à l'autre et on ne consignait pas toujours la communication ou la réception d'information en vertu de la LCISC. Par conséquent,

les institutions ne nous ont pas toutes fourni des documents complets de données rapprochés sur leurs activités de communication d'information en vertu de la Loi. Le Commissariat n'a donc pas été en mesure d'examiner toute l'ampleur de la communication d'information en vertu de la LCISC et ne pouvait évaluer que toute cette activité était entièrement en conformité avec la *Loi sur la protection des renseignements personnels.*

Cependant, pour une majorité des dossiers que nous avons été en mesure d'examiner, l'information avait été communiquée en réponse à une demande officielle de renseignements concernant des individus qui faisaient l'objet d'une enquête et l'information en question ne dépassait pas les paramètres de la demande. Nous avons aussi constaté que bon nombre des communications proactives avaient été précédées d'une discussion entre les deux institutions participant à l'échange d'information. Il ne s'agit pas d'un problème systémique, mais nous avons vu des cas où une institution avait communiqué de l'information au sujet de membres de la famille d'individus faisant l'objet d'une enquête, alors que rien ne prouvait que cette information respectait le seuil de pertinence prévu par la LCISC.

Principales observations :

- Les registres sont incomplets et aucune structure officielle n'est en place pour assurer le suivi et la surveillance de l'échange d'information en vertu de la LCISC.
- Aucune activité de gestion du risque n'a été menée pour détecter et atténuer les risques d'atteinte à la vie privée liés à la mise en œuvre et au mode d'application de la LCISC.
- Il faut améliorer certains mécanismes de contrôle interne pour assurer un traitement approprié des renseignements personnels.

En analysant l'ensemble de nos constatations, nous avons observé que bon nombre de nos préoccupations initiales concernant la LCISC demeurent pertinentes. En l'absence de registres uniformes et officiels des activités de communication d'information dans l'ensemble du gouvernement et de mécanismes de contrôle interne rigoureux, le risque de communication excessive et non autorisée de renseignements personnels persiste. Le seuil pour la communication d'information avait été respecté dans la grande majorité des dossiers que nous avons examinés, mais la norme de pertinence prévue par la LCISC est extrêmement faible. La Loi prévoit un seuil très bas et elle ne renferme aucune disposition sur le traitement approprié de l'information susceptible d'être communiquée, si bien qu'il est tout à fait possible que les organisations l'invoquent pour communiquer des renseignements au sujet d'individus qui pourraient ne jamais représenter une menace pour la sécurité du Canada.

On trouvera tous les détails de nos observations et recommandations ainsi que la réponse de l'organisation dans le rapport sur la mise en œuvre de la LCISC.

Examen des efforts de la GRC pour lutter contre la radicalisation menant à la violence

Le Livre vert du gouvernement du Canada traite des efforts déployés pour lutter contre la « radicalisation menant à la violence ». Dans le mémoire que nous avons déposé en réponse à ce document, nous reconnaissons la valeur de ces efforts, tout en précisant que nous trouverions préoccupant que les activités de prévention à cet égard comprennent une surveillance généralisée de la navigation dans Internet. Nous avons préconisé une approche qui oriente les activités de prévention ou les efforts de détection vers les menaces crédibles révélées par des renseignements fiables. C'est dans cet esprit que nous avons mené les enquêtes préliminaires sur le Programme de prévention du terrorisme (PPT) de la GRC en février 2017.

Dans le cadre du PPT, l'Équipe intégrée de la sécurité nationale de la GRC apporte un soutien aux enquêtes relatives à la sécurité nationale concernant des individus radicalisés devenus violents mais sans atteindre le seuil de criminalité voulu pour que la mise en accusation soit approuvée. Une évaluation

est effectuée, au moyen d'un éventail d'outils, pour déterminer la probabilité de réussite d'une intervention. L'Équipe intégrée de la sécurité nationale joue un rôle de soutien, mais elle n'assume aucune fonction d'enquête.

La GRC a confirmé qu'elle n'utilise aucune technique ni aucune technologie de surveillance de masse dans le cadre de ses efforts visant à détecter et à prévenir les menaces pour la sécurité nationale, qu'elle n'exerce pas de surveillance à grande échelle de la navigation dans Internet et qu'elle n'effectue aucun ciblage fondé sur des scénarios. Elle ouvre plutôt ses enquêtes sur la sécurité nationale sur la base d'information de différentes sources, notamment les membres de la famille, le grand public ou les partenaires de la GRC chargés de la sécurité et de l'application de la loi.

Examen du ciblage des voyageurs fondé sur des scénarios de l'ASFC—Sécurité nationale

En vertu du droit canadien[9], tous les transporteurs aériens commerciaux doivent transmettre à l'Agence des services frontaliers du Canada (ASFC) l'information préalable sur les voyageurs et l'information du dossier passager (IPV-DP) pour chaque personne qui voyage au Canada, notamment son nom, sa date de naissance, sa citoyenneté, ses numéros de téléphone, son numéro de siège et l'information sur le paiement. L'ASFC utilise ces données pour identifier les personnes qui ont commis ou qui sont susceptibles de commettre des actes terroristes, des crimes liés au terrorisme ou d'autres crimes graves de nature transnationale. Le programme de ciblage fondé sur des scénarios (PCFS) utilise l'analytique avancée pour évaluer les données ainsi recueillies par rapport à un ensemble de conditions ou de scénarios.

Les scénarios prennent en compte des caractéristiques personnelles provenant de l'IPV-DP, comme l'âge, le sexe, le pays émetteur des titres de voyage, les endroits visités ainsi que la durée des séjours et les habitudes de voyage. Si une personne correspond à un scénario, les agents du Centre national de ciblage effectuent des évaluations supplémentaires du risque—qui comprennent la vérification des caractéristiques de la personne dans les bases de données de partenaires canadiens et internationaux chargés du renseignement et de l'application de la loi ainsi que des recherches dans des bases de données ouvertes. À l'issue de ces vérifications, la personne pourrait être identifiée comme « cible » et subir un interrogatoire ou un examen approfondi mené par un agent des services frontaliers au point d'entrée.

Notre examen avait pour but de déterminer si l'ASFC avait mis en place des mécanismes de contrôle adéquats—notamment des politiques et des procédures—pour s'assurer que les pratiques de traitement des renseignements personnels dans le cadre du PCFS sont conformes à la *Loi sur la protection des renseignements personnels* et aux politiques, directives et orientations connexes du gouvernement du Canada. Nous nous sommes concentrés sur les scénarios élaborés à des fins de sécurité nationale et sur un échantillon de dossiers de personnes ciblées entre le 31 janvier 2016 et le 31 janvier 2017.

Nous avons conclu que l'ASFC avait mis en place des politiques et des procédures pour orienter l'élaboration et l'amélioration de scénarios, le processus d'évaluation des risques liés aux personnes et l'évaluation de l'efficacité des scénarios. Toutefois, certains scénarios sont rédigés de manière si générale qu'un nombre élevé de personnes—environ 60 000 par année—sont ciblées en vue d'un examen approfondi en fonction de facteurs comme l'âge, le sexe, le pays d'origine et les habitudes de voyage. Sur ce nombre, seul un petit groupe doit se soumettre à un examen plus approfondi après que les personnes

9 L'obligation de fournir l'information préalable sur les voyageurs est prévue aux alinéas 5a) à d) et f) du Règlement sur les renseignements relatifs aux passagers (douanes) pris en application de la Loi sur les douanes, et aux alinéas 269(1)a) à d) et f) du Règlement sur l'immigration et la protection des réfugiés pris en application de la Loi sur l'immigration et la protection des réfugiés.

aient été ciblées. Durant la période visée par l'examen, ce nombre se chiffrait à 552 personnes.

Nous reconnaissons l'importance d'un programme visant à évaluer les personnes qui arrivent au Canada afin de repérer les individus qui pourraient représenter une menace pour la sécurité nationale, mais il s'avère que la grande majorité des personnes correspondant à un scénario ne représentaient aucune menace. Toutefois, leurs renseignements personnels ont été recueillis, évalués et communiqués à certains partenaires canadiens et internationaux de l'ASFC chargés du renseignement et de l'application de la loi dans le cadre du processus d'évaluation des risques. En outre, l'ASFC reconnaît la nécessité d'évaluer les scénarios afin d'en déterminer l'incidence possible sur la vie privée, les droits de la personne et les libertés civiles. Or, les scénarios de sécurité nationale ont été mis en place sans avoir fait l'objet d'un tel examen.

Nous avons également constaté les faits suivants :

- Les protocoles d'entente conclus avec les partenaires canadiens et internationaux de l'ASFC ne contiennent aucune disposition précise limitant la conservation et l'utilisation des données communiquées par l'ASFC à des fins de vérification des bases de données, particulièrement pour atténuer le risque de soupçons continus à l'égard des personnes considérées comme ne représentant aucune menace pour la sécurité nationale.
- L'ASFC mesure le succès de ses scénarios de sécurité nationale en fonction d'un vaste éventail de critères, entre autres les résultats intermédiaires, qui ne se limitent pas aux résultats liés à la sécurité nationale.
- Certains renseignements personnels qui n'ont aucun lien direct avec l'objectif déclaré du programme, particulièrement ceux provenant des médias sociaux et concernant des tiers, sont recueillis et conservés dans les systèmes de l'ASFC.

Nous sommes heureux de constater que l'ASFC a accepté l'ensemble de nos recommandations.

Le 26 juillet 2017, la Cour de justice de l'Union européenne (CJUE) a rendu son avis concernant la compatibilité d'un accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (PNR). L'accord avait été signé en 2014, mais le Parlement européen a par la suite demandé à la CJUE de statuer sur sa compatibilité avec le droit de l'Union européenne, notamment en ce qui concerne le respect du droit à la vie privée et la protection des données personnelles. Dans son avis, la CJUE a souligné que l'accord ne respectait pas les exigences de nécessité et de proportionnalité prévues par la loi, particulièrement en ce qui a trait à la conservation des renseignements de personnes qui, d'après l'évaluation, ne présentent aucune menace pour la sécurité nationale. La CJUE a conclu que les dispositions de l'accord portant sur le transfert des données sensibles au Canada ainsi que sur le traitement et la conservation de ces données étaient incompatibles avec les droits fondamentaux. En bout de ligne, la CJUE a déterminé que l'accord ne pouvait être conclu sous sa forme actuelle et elle a souligné plusieurs dispositions qui devraient figurer dans un accord révisé.

Cet avis a aussi mis en évidence l'importance de s'assurer que des limites strictes sont établies pour la conservation et l'utilisation de l'information préalable sur les voyageurs ou des données PNR et d'autres renseignements personnels recueillis ultérieurement par l'ASFC aux fins de l'administration du PCFS, particulièrement dans le cas des personnes qui, d'après l'évaluation, ne présentent aucune menace pour la sécurité nationale.

On trouvera tous les détails de nos observations et recommandations ainsi que la réponse de l'organisation dans le rapport intégral de l'examen du ciblage des voyageurs fondé sur des scénarios de l'ASFC.

Examen du Centre d'analyse des données opérationnelles du SCRS

En 2006, le Service canadien du renseignement de sécurité (SCRS) a mis sur pied le Centre d'analyse des données opérationnelles (CADO). Ce centre apporte son soutien à plusieurs divisions opérationnelles du SCRS en analysant et en exploitant les données recueillies, entre autres, en vertu d'un mandat conformément à l'article 21 de la *Loi sur le Service canadien du renseignement de sécurité.* Il génère des produits d'information en établissant des liens entre l'information tirée de plusieurs sources et banques de données.

Dans le cadre de l'exécution de mandats délivrés par un tribunal contre des individus qui représentent une menace pour la sécurité, le SCRS recueille le contenu de leurs communications ainsi que leurs métadonnées, parfois appelées « données associées ». Au sens large, les métadonnées sont des renseignements au sujet d'une communication.

Depuis la création du CADO en 2006, le SCRS y a stocké toutes les métadonnées recueillies, sans égard au fait que le contenu de la communication originale ait été conservé ou non. Dans une décision rendue en octobre 2016, la Cour fédérale a conclu que le SCRS avait conservé illégalement des métadonnées de tiers non liées à une menace. Les renseignements sur les tiers concernent des individus qui ne sont pas visés par une enquête du SCRS, tandis que les renseignements non liés à une menace sont ceux ne se rapportant pas à « une menace envers la sécurité du Canada » au sens de l'article 2 de la *Loi sur le Service canadien du renseignement de sécurité*.

La décision de la Cour fédérale était manifestement une décision importante pour le droit à la vie privée et l'avancement de la protection des renseignements personnels. Dans sa réponse, le SCRS a indiqué qu'il interdirait l'accès aux métadonnées en question jusqu'à ce qu'il ait examiné la décision de la Cour. Le SCRS a aussi demandé à discuter avec le Commissariat à la protection de la vie privée du Canada. Le ministre de la Sécurité publique a confié au Comité de surveillance des activités de renseignement de sécurité (CSARS) le mandat de superviser le blocage et le contrôle de l'accès aux métadonnées en question.

Notre examen portait principalement sur les mesures prises par le SCRS à la suite de la décision du tribunal concernant la conservation, par le CADO, des métadonnées sur des tiers non liées à une menace. Nous avons confirmé que les banques de métadonnées historiques du CADO étaient bloquées et que les analystes du CADO n'y auraient pas accès avant la décision finale relative à la disposition des données. En outre, nous avons été en mesure de constater la mise sous séquestre des métadonnées dans le système du CADO, mais nous avons appris que ces renseignements étaient stockés ailleurs dans des dossiers de sauvegarde du SCRS. Tous les efforts sont mis en œuvre pour veiller à ce que toutes les données visées soient retirées conformément à la décision de la Cour.

Nous nous sommes aussi renseignés sur la gestion future des métadonnées dans le système du CADO. Nous avons examiné les règles imposées par la Cour concernant l'évaluation des données sur des tiers et les mesures prévues par le SCRS pour appliquer ces règles. Ces travaux étaient en cours pendant la rédaction du présent rapport mais, d'après notre examen, ces mesures sont conformes à la décision de la Cour. Soulignons que le projet de loi C-59, déposé à la Chambre des communes le 20 juin 2017, renferme des dispositions sur la collecte, la conservation et l'utilisation d'ensembles de données—ce qui comprend les métadonnées—par le SCRS. Il prévoit notamment qu'une autorisation précise soit exigée pour conserver des ensembles de données auxquels le public n'a pas accès. Selon la nature des données, le ministre de la Sécurité publique, un nouveau commissaire au renseignement et le tribunal accorderait cette autorisation. Il est trop tôt pour

savoir ce qu'il adviendra du projet de loi mais, en attendant, les mesures prévues par le SCRS nous semblent à première vue respecter la décision de la Cour.

Suivi de l'examen de 2014 portant sur l'accès sans mandat aux renseignements des abonnés

Au cours de l'exercice, nous avons fait le suivi de notre Examen de la Gendarmerie royale du Canada 2014—Accès sans mandat aux renseignements des abonnés afin de déterminer si la GRC avait mis en place des mécanismes lui permettant de surveiller la collecte de renseignements sur les abonnés et d'en rendre compte, comme nous l'avions recommandé. Ces mécanismes favoriseront une plus grande transparence concernant les demandes présentées sans mandat par la GRC aux fournisseurs de services de télécommunication afin d'obtenir des renseignements de base sur les abonnés (RBA).

La GRC a déclaré avoir mis sur pied, après la publication de notre rapport en octobre 2014, un groupe de travail chargé d'examiner les difficultés liées à l'accès sans mandat aux RBA. Depuis la décision rendue par la Cour suprême du Canada dans R. c. Spencer, elle demande des RBA sans ordonnance de communication uniquement lorsque des circonstances contraignantes l'exigent.

Un groupe de travail fédéral, provincial et territorial sur la cybercriminalité, qui a mené des consultations auprès de membres de la société civile dans le cadre de ses travaux, a aussi étudié la question des RBA et les répercussions de la décision *Spencer*. Ce groupe de travail a été chargé de trouver des solutions possibles pour assurer un accès uniforme, rapide et adéquat des organismes d'enquête aux RBA. Les résultats n'ont pas encore été soumis à l'examen du gouvernement.

Étant donné que les RBA sont fournis uniquement dans des circonstances contraignantes et que le gouvernement étudie encore les répercussions de la décision *Spencer* et les solutions possibles, la GRC nous a informés qu'elle reporterait sa réponse à notre recommandation jusqu'à ce que le gouvernement du Canada ait déterminé l'approche globale qu'il adoptera en ce qui concerne les rapports de transparence afin de ne pas mettre en œuvre une stratégie allant à l'encontre des futurs objectifs du gouvernement.

Nous constatons que les demandes présentées sans mandat par la GRC dans des circonstances contraignantes ne font l'objet d'aucun suivi distinct et ne sont pas rendues publiques. Par conséquent, il subsiste une lacune dans les rapports de transparence du secteur public, et les organisations du secteur privé ne fournissent que des renseignements limités sur la fréquence à laquelle elles exercent ce pouvoir, qui porte atteinte à la vie privée. Plus de trois ans se sont écoulés depuis l'arrêt *Spencer* et les Canadiens attendent toujours l'adoption d'une approche moderne à l'égard des rapports de transparence. Nous poursuivrons le suivi de cette question auprès de la GRC.

Par ailleurs, il est important de souligner que nos recommandations sur la réforme de la *Loi sur la protection des renseignements personnels* préconisent notamment que les organisations fédérales soient tenues de faire preuve de transparence en communiquant le nombre de demandes d'accès licite à des renseignements personnels qu'elles adressent à des fournisseurs d'accès Internet et à d'autres organisations du secteur privé auxquels sont confiés des renseignements de clients et en précisant la fréquence et la nature de ces demandes.

Protection des Canadiens à la frontière

Les voyageurs qui passent par un aéroport canadien ou franchissent un poste frontalier américain font l'objet d'une surveillance rigoureuse et de plusieurs niveaux de mesures de sécurité. En effet, les aéroports, les ports de mer, les voies maritimes internationales et les postes frontaliers terrestres diffèrent grandement des autres lieux publics au Canada, car les attentes en matière de protection de la vie privée y sont moindres. Mais cela ne signifie pas que les voyageurs perdent alors tout droit à leur vie privée.

Les Canadiens expriment de plus en plus de préoccupations concernant leurs droits dans ces situations. Le Commissariat a publié une fiche d'information sur le droit à la vie privée dans les aéroports et aux postes frontaliers, qui indique aux voyageurs à quoi s'attendre et à qui s'adresser s'ils estiment que leur droit à la vie privée a été bafoué. La fiche d'information a été largement consultée sur notre site Web, surtout au cours des derniers mois.

Fouille d'appareils électroniques aux postes frontaliers canadiens et américains

Nous avons reçu récemment plusieurs plaintes d'individus alléguant que des agents des services frontaliers canadiens leur avaient demandé de remettre leurs appareils électroniques—téléphone intelligent, tablette électronique ou ordinateur portable—à des fins d'inspection, souvent en exigeant leur mot de passe pour avoir accès au contenu.

En règle générale, les agents de l'ASFC aux postes frontaliers possèdent de vastes pouvoirs pour intercepter et fouiller des individus et examiner leurs bagages et autres effets personnels. En vertu de la *Loi sur les douanes* du Canada, ils peuvent exercer ces pouvoirs sans mandat.

Les tribunaux canadiens reconnaissent généralement que les voyageurs ont des attentes réduites en matière de protection de la vie privée aux postes frontaliers. Dans ce contexte, le droit à la vie privée et les autres droits garantis par la Charte s'appliquent toujours, mais ils sont limités par les impératifs de l'État—souveraineté nationale, contrôle de l'immigration, fiscalité, protection du public et sécurité. Le droit est imprécis, mais la politique de l'ASFC prévoit que les appareils personnels ne doivent pas être examinés de manière systématique; ces fouilles doivent être menées uniquement s'il y a des indications ou des motifs selon lesquels les appareils ou les supports numériques pourraient contenir la preuve d'infractions.

Cela dit, notre enquête portant sur ces plaintes est en cours et nous présenterons nos conclusions en temps voulu.

Nous avons aussi reçu plusieurs questions dernièrement concernant ce à quoi les Canadiens qui se rendent aux États-Unis peuvent s'attendre à la frontière. De nombreux voyageurs ont déclaré que les agents de la U.S. Customs and Border Protection (CBP) leur avaient fait subir un interrogatoire poussé et avaient exigé le mot de passe de leurs appareils électroniques. Nous avons averti les voyageurs de limiter les objets qu'ils apportent ou de supprimer les renseignements sensibles stockés sur des appareils susceptibles d'être fouillés.

Projet de loi C-23—Loi sur le précontrôle de 2016

En juin 2016, le gouvernement a déposé le projet de loi C-23, *Loi sur le précontrôle* de 2016. Ce projet de loi visait à mettre en œuvre les modalités de l'Accord entre le gouvernement du Canada et le gouvernement des États-Unis relatif au précontrôle dans les domaines du transport terrestre, ferroviaire, maritime et aérien, conclu en mars 2015. Il s'agissait essentiellement d'élargir la portée des dispositions existantes en vertu desquelles les voyageurs et les biens à destination des États-Unis peuvent faire l'objet d'un précontrôle au Canada et inversement. Soulignons qu'en vertu du projet de loi C-23, les contrôleurs américains au Canada doivent avoir des motifs raisonnables de

soupçonner des personnes pour effectuer une fouille corporelle, y compris la fouille par palpation, qui est relativement non intrusive.

Le Commissariat s'inquiète du projet de loi sous sa forme actuelle, à la lumière des récentes déclarations de l'administration américaine selon lesquelles elle a l'intention de fouiller, à sa discrétion et sans motif juridique, les appareils électroniques des étrangers qui souhaitent entrer aux États-Unis. En fait, comme il a été mentionné, cette situation semble déjà se produire : on demande aux personnes de fournir le mot de passe de leur téléphone ou de leurs comptes de médias sociaux. Nous nous inquiétons entre autres car il semble que cette politique s'appliquerait dans des zones de précontrôle en sol canadien.

La politique canadienne, en revanche, prévoit ce type de fouille uniquement s'il y a des motifs ou des indications selon lesquels les appareils ou les supports numériques pourraient contenir la preuve d'infractions. La fouille d'un appareil électronique constitue une procédure extrêmement envahissante sur le plan de la vie privée. La Cour suprême du Canada l'a reconnu à plusieurs occasions. L'idée selon laquelle les appareils électroniques devraient être considérés comme de simples biens et, par conséquent, pouvoir faire l'objet de fouilles sans motif juridique à la frontière est certainement dépassée et elle ne reflète pas les réalités de la technologie moderne. C'est pourquoi nous avons recommandé au Parlement, en juin 2017, de modifier le projet de loi C-23 pour traiter la fouille d'appareils électroniques aux postes frontaliers de la même façon que la fouille de personnes. Ainsi, un motif raisonnable de soupçonner un acte répréhensible serait obligatoire pour effectuer ce type de fouille.

Comme pour ce qui est de l'Accord relatif au précontrôle, le projet de loi C-23 obligerait les contrôleurs à respecter les lois du pays d'accueil lorsqu'ils s'y trouvent. Ainsi, les agents de l'ASFC travaillant aux États-Unis devraient se conformer au droit américain, tandis que les contrôleurs de la U.S. Customs and Border Protection (CBP) travaillant au Canada devraient se conformer au droit canadien, notamment à la *Charte canadienne des droits et libertés*, à la *Déclaration canadienne des droits* et à la *Loi canadienne sur les droits de la personne*.

Toutefois, ces protections sont quelque peu inopérantes. Selon l'article 39 du projet de loi, les procédures civiles intentées contre les États-Unis seraient assujetties à la *Loi sur l'immunité des États* de 1985. Cette disposition limite considérablement les recours civils contre les États-Unis pour des actes posés par des contrôleurs du CBP dans l'exercice de leurs fonctions de précontrôle au Canada. Dans bien des cas, toutefois, il semble que les Canadiens qui souhaitent se rendre aux États-Unis devront faire un choix difficile dans les zones de précontrôle au Canada et aux postes frontaliers aux États-Unis, c'est-à-dire accepter que leurs appareils soient fouillés sans motif juridique ou renoncer à entrer aux États-Unis.

Lettre faisant suite au décret présidentiel

À la suite de l'émission d'un décret par le président des États-Unis, Donald Trump, en janvier 2017, nous avons reçu plusieurs demandes concernant les répercussions possibles de ce décret sur les Canadiens. En vertu du décret, les organismes gouvernementaux américains, dans la mesure où les lois applicables le permettent, doivent veiller à ce que leurs politiques de protection de la vie privée excluent les personnes qui ne sont pas des citoyens américains ni des résidents permanents de la protection offerte par la *Privacy Act* des États-Unis.

En bref, nous avons constaté que même si la vie privée des Canadiens bénéficie d'une certaine protection aux États-Unis, cette protection est précaire du fait qu'elle repose principalement sur des ententes administratives n'ayant pas force de loi. Dans une lettre adressée aux ministres de la Justice, de la Sécurité publique et de la Protection civile ainsi que de la Défense nationale, le commissaire a demandé quelles pourraient être les

répercussions de la mise en œuvre du décret sur les dispositions relatives à la protection de la vie privée figurant dans ces ententes. Par exemple, les Canadiens veulent savoir—et ils en ont le droit—si les États-Unis respecteront toujours les dispositions de cette nature énoncées dans le plan d'action *Par-delà la frontière* et l'accord du Groupe des cinq.

Le commissaire a aussi exhorté le gouvernement à demander que le Canada soit ajouté à la liste des pays désignés par la *Judicial Redress Act* des États-Unis. Cette désignation, qui s'applique déjà à 26 pays européens, permet à leurs citoyens de faire valoir certains droits relatifs à la vie privée en s'adressant aux tribunaux américains.

Au moment de la rédaction du présent rapport, le commissaire attendait toujours une réponse des ministres.

Enquêtes sur la sécurité nationale, sécurité publique et protection de la vie privée à la frontière

En 2016-2017, nous avons mené à bien plusieurs enquêtes sur des plaintes déposées par des individus alléguant que des organismes fédéraux chargés de la sécurité nationale avaient abusé des droits que leur confère la *Loi sur la protection des renseignements personnels*. On trouvera ci-après le résumé des conclusions de plusieurs de ces enquêtes et à la page 79 le rapport de conclusions d'autres enquêtes menées en vertu de la *Loi sur la protection des renseignements personnels*.

Centre d'information de la police canadienne de la GRC—Communication de renseignements sur la santé mentale de Canadiens aux autorités américaines

Une personne a allégué que la GRC avait communiqué de façon inacceptable aux autorités frontalières des États-Unis, par l'intermédiaire du Centre d'information de la police canadienne (CIPC), des renseignements concernant une tentative de suicide. La U.S. Customs and Border Protection (CBP) a par la suite interdit l'accès de la plaignante aux États-Unis sur la base de ces renseignements.

Les renseignements concernant la tentative de suicide de la plaignante avaient été téléchargés dans la base de données du CIPC par le Service de police de Toronto (SPT), qui était intervenu lorsque la plaignante avait appelé le 911. Nous avons constaté que certains types de renseignements, une fois stockés dans la base de données du CIPC, sont communiqués aux organismes d'application de la loi américains en vertu d'une entente de coopération entre la GRC et le Federal Bureau of Investigation (FBI). Nous estimons qu'il incombe à la GRC, en tant que partie à l'entente et administratrice du CIPC, de s'assurer que la communication de renseignements entre les organismes canadiens et américains est conforme aux exigences énoncées dans les politiques du CIPC et l'entente de coopération. En outre, nous considérons que le niveau de contrôle exercé par la GRC sur le CIPC lui impose la responsabilité de s'assurer que la communication de tous les renseignements personnels aux organismes d'application de la loi américains par l'intermédiaire du CIPC est conforme à la *Loi sur la protection des renseignements personnels*.

En examinant l'entente de coopération et les politiques du CIPC, nous avons constaté que les renseignements du CIPC « appartiennent » à l'organisme contributeur—dans le cas présent, le SPT—et que seul cet organisme a le pouvoir d'autoriser l'utilisation des renseignements qu'il a fournis. La GRC a confirmé que cette exigence n'avait pas été respectée, car un agent du CBP avait utilisé les renseignements personnels de la plaignante sans avoir obtenu au préalable l'autorisation du SPT ni vérifié l'exactitude des renseignements.

Nous avons constaté que la communication des renseignements personnels de la plaignante n'était pas autorisée en vertu de la *Loi sur la protection*

des renseignements personnels. Le CBP a utilisé ces renseignements pour une évaluation de l'admissibilité ne cadrant pas avec les fins pour lesquelles le SPT les avait obtenus ou compilés, soit aider les policiers à effectuer une intervention appropriée au cas où ils traiteraient de nouveau le dossier de la plaignante dans le cadre de leurs activités de maintien de l'ordre. Nous avons conclu que les renseignements relatifs à une tentative de suicide peuvent être communiqués aux autorités frontalières des États-Unis seulement si l'on peut raisonnablement considérer que l'individu présente un risque pour d'autres personnes. Or, rien n'indiquait que la plaignante constituait une menace pour la sécurité publique. Nous avons donc conclu que la plainte était fondée.

À la suite de nombreux échanges avec la GRC au cours de cette enquête, plusieurs modifications ont été apportées aux politiques et au système du CIPC. Nous avons fait parvenir à la GRC notre rapport de conclusions final, dans lequel nous recommandons d'autres modifications à apporter au système et aux politiques du CIPC. En janvier 2017, la GRC a fait savoir qu'elle n'était d'accord ni avec les conclusions du Commissariat ni avec ses recommandations. De manière générale, elle se dit d'avis que [traduction] « le rapport de conclusions n'aborde pas le devoir crucial et le rôle de la police de protéger les individus, y compris contre eux-mêmes ».

Nous reconnaissons l'importance du CIPC, lequel permet aux partenaires chargés de l'application de la loi et de la sécurité publique de collaborer efficacement. Nous sommes d'accord avec la GRC sur le fait que, dans certaines circonstances, la communication de renseignements liés à une tentative de suicide peut cadrer avec les obligations en droit commun des policiers de maintenir la paix, de prévenir la criminalité, de mener des enquêtes criminelles et de protéger la vie et les biens. Cependant, nous estimons que l'évaluation de l'admissibilité à laquelle a procédé le CBP dans les circonstances ne cadrait pas avec ces fins et qu'il faudrait mettre en place des mécanismes de contrôle supplémentaires afin de limiter la communication de renseignements sensibles et qui ne sont pas liés à des actes criminels aux autorités frontalières américaines.

Il est à noter que nos conclusions concordent avec celles formulées par le commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVPO) dans son rapport intitulé *Crossing the Line : the Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CIPC*. Plus particulièrement, nous approuvons « le critère de communication de renseignements sur la santé mentale » proposé dans ce rapport publié en avril 2014. Ce critère décrit les circonstances dans lesquelles, selon le CIPVPO, la communication de renseignements personnels liés à une tentative de suicide serait justifiée. La GRC estime que ce critère est de portée trop restreinte du fait qu'il n'autorise pas la communication de renseignements lorsqu'un individu pourrait constituer un danger pour lui-même plutôt que pour les autres, mais nous constatons en revanche que le SPT a mis en œuvre en août 2015 de nouvelles pratiques fondées sur le critère de communication de renseignements sur la santé mentale et plusieurs autres recommandations formulées dans le rapport du CIPVPO.

Capteurs IMSI

Nous avons fait enquête sur une plainte déposée par OpenMedia concernant le refus de la GRC de confirmer ou d'infirmer qu'elle utilise des simulateurs de sites cellulaires (aussi appelés « dispositifs Stingray » ou « capteurs IMSI ») dans le cadre de ses activités de surveillance, tel que rapporté par divers médias. En règle générale, nous dissimulons l'identité des plaignants, mais dans ce dossier, OpenMedia a publié un communiqué et nous a autorisés explicitement à communiquer cette information.

Le plaignant craignait particulièrement que la GRC se serve de ce type d'appareils pour surveiller de grands groupes d'individus à un endroit donné. Il craignait

aussi que les appareils permettent d'intercepter le contenu des communications vocales et des messages textes et d'extraire les clés de chiffrement utilisées pour protéger les données sur les appareils électroniques personnels. De l'avis du plaignant, le public est en droit d'être informé de l'utilisation de ces technologies, le cas échéant, puisqu'elles pourraient donner lieu à des atteintes à la vie privée de Canadiens innocents, à leur insu ou sans leur consentement.

En avril 2017, la GRC a tenu une « séance d'information technique » à l'intention de plusieurs médias. Elle a alors confirmé qu'elle possède et utilise effectivement dans certains types d'enquêtes des simulateurs de sites cellulaires, appelés « identificateurs d'appareils mobiles ». En gros, la GRC a expliqué que :

- son utilisation de simulateurs de sites cellulaires est conforme aux lois canadiennes, entre autres la *Charte canadienne des droits et libertés*, le *Code criminel du Canada* et les processus judiciaires appropriés établis devant les tribunaux par la jurisprudence ou la common law;
- les renseignements personnels recueillis à l'aide des simulateurs de sites cellulaires qu'elle utilise comprennent uniquement le numéro d'identité internationale d'abonnement mobile (IMSI) et celui d'identité internationale d'équipement mobile (IMEI) associés aux téléphones cellulaires—qui sont des numéros uniques normalisés permettant d'identifier respectivement l'abonné et l'appareil. Les simulateurs ne permettent pas de capter les communications privées, notamment les communications vocales ou audio, les courriels, les messages texte, les listes de contacts, les images, les clés de chiffrement ou les renseignements de base sur l'abonné.

Les renseignements fournis aux médias par la GRC concordaient avec les observations déjà formulées au Commissariat dans le cadre de son enquête. C'est pourquoi nous avons procédé en toute indépendance à une vérification des capacités techniques des simulateurs de sites cellulaires de la GRC et demandé des renseignements complémentaires sur les lois en vertu desquelles ils sont exploités et sur les méthodes employées par la GRC pour utiliser, conserver et éliminer les données recueillies au moyen de ces appareils.

La GRC nous a informés qu'elle avait déployé des identificateurs d'appareils mobiles dans le cadre de 125 enquêtes criminelles au cours des cinq années précédentes, soit de 2011 à 2016. Sur ce nombre, 91 déploiements avaient été autorisés en vertu d'un mandat général et 22 en vertu d'un mandat pour un enregistreur de données de transmission. Aucune autorisation judiciaire n'avait été obtenue dans le cas de 13 déploiements, mais la GRC a précisé que des circonstances contraignantes exigeaient le déploiement des appareils dans sept de ces cas. En droit criminel canadien, il y a des « circonstances contraignantes » lorsqu'un policier a des motifs de croire qu'une intervention particulière est nécessaire afin de prévenir la perte ou la destruction imminentes d'un élément de preuve, des lésions corporelles imminentes ou une mort imminente. Il se peut qu'un mandat ne soit pas nécessaire dans ces circonstances. La GRC a affirmé avoir suivi au moment du déploiement dans les six autres cas un avis juridique selon lequel aucun mandat n'était requis pour déployer les identificateurs d'appareils mobiles.

La GRC a fait une démonstration de l'utilisation des identificateurs d'appareils mobiles et nous a autorisés à les inspecter. Nous avons pu constater que les identificateurs utilisés ne permettent pas de capter les communications privées, comme les communications vocales, les courriels, les messages textes, les listes de contacts, les images, les clés de chiffrement ou les renseignements de base sur l'abonné. Nous savons aussi que dans les cas où la GRC avait obtenu une autorisation judiciaire préalable, les renseignements personnels recueillis au moyen des identificateurs d'appareils mobiles respectaient les exigences de la *Loi sur la protection des renseignements personnels* et

qu'ils ont été isolés, sécurisés et, finalement, détruits de manière appropriée. Un mandat que nous a fourni la GRC à titre d'exemple corrobore nos conclusions. On y précise que tous les renseignements personnels recueillis au moyen de l'identificateur d'appareils mobiles seront protégés contre toute utilisation ou communication à quelque fin que ce soit, sauf en cas d'ordonnance contraire d'un tribunal compétent. Nous estimons que ces modalités offrent une importante mesure de protection des renseignements personnels recueillis au moyen de ces appareils. Toutefois, dans les six dossiers où la GRC n'avait obtenu aucun mandat et où il n'y avait pas de circonstances contraignantes, nous estimons que la collecte de renseignements personnels contrevenait à la *Loi sur la protection des renseignements personnels*.

Nous avons donc conclu que la plainte était non fondée dans les cas où le déploiement des identificateurs d'appareils mobiles avait été autorisé par un mandat. Toutefois, dans les six dossiers où la GRC n'avait obtenu aucun mandat—et en l'absence de circonstances contraignantes –, la plainte était fondée. Nous sommes d'avis que la GRC agissait de bonne foi sur la base des avis juridiques obtenus, mais nous ne croyons pas que le déploiement des identificateurs d'appareils mobiles ait été conforme à la loi dans ces six cas.

Même si nous avons conclu que la plainte était fondée dans le cas de six déploiements, nous estimons que la GRC a pris des mesures appropriées pour remédier à la situation. En effet, elle exige dorénavant une autorisation judiciaire préalable pour tout déploiement d'identificateurs d'appareils mobiles, à moins qu'il y ait des circonstances contraignantes, auquel cas aucun mandat ne serait requis. Des renseignements supplémentaires figurent dans le rapport de conclusions sur les capteurs IMSI.

Nous poursuivons aussi notre enquête sur une autre plainte alléguant que, selon plusieurs reportages dans les médias, Service correctionnel Canada (SCC) a utilisé des capteurs IMSI à l'établissement de Warkworth, en Ontario.

Commission des libérations conditionnelles du Canada—Refus d'accès

Au Canada, un individu souhaitant travailler ou faire du bénévolat dans un contexte qui le placerait en situation de confiance ou d'autorité vis-à-vis de personnes vulnérables—comme des enfants, des personnes âgées ou des personnes handicapées—peut devoir se soumettre à une vérification des antécédents en vue d'un travail auprès de personnes vulnérables (VAPV). Cette vérification approfondie du casier judiciaire permet notamment de déterminer si un individu a bénéficié d'une suspension de son casier judiciaire (auparavant appelée « réhabilitation ») associée à certaines infractions de nature sexuelle. Ce type d'information ne ressort pas d'une vérification de base du casier judiciaire.

En vertu de la *Loi sur le casier judiciaire,* la VAPV peut être obtenue auprès d'un service de police. Le service de police envoie les empreintes digitales de l'individu à la Gendarmerie royale du Canada (GRC), qui vérifiera s'il a bénéficié d'une suspension de son casier judiciaire pour une infraction pertinente. Le délai d'attente pour une VAPV dépasse parfois plusieurs mois, ce qui peut entraîner la perte de possibilités d'emploi, d'occasions de bénévolat ou de placement étudiant. Ultimement, dans certains cas, des citoyens admissibles ne pourront donc pas participer pleinement à des activités.

Pour accélérer le processus de vérification de ses clients, une entreprise canadienne de vérification des antécédents a élaboré un outil de vérification offrant une solution de rechange au long processus de VAPV. Ce nouvel outil comprend la présentation d'une demande d'accès à des renseignements personnels *à la Commission des libérations conditionnelles du Canada (CLCC)* en vertu de la *Loi sur la protection des renseignements personnels*. Une réponse de la CLCC indiquant qu'elle ne détient aucun dossier sur le demandeur serait utile pour le processus de vérification, puisque la CLCC tient un dossier pour les personnes qui ont obtenu une suspension de leur casier.

Après avoir été inondée de demandes, la CLCC a cessé de les traiter en invoquant une exception prévue par la *Loi sur la protection des renseignements personnels*. En effet, en vertu de l'alinéa 22(1)*b*) de la Loi, une institution gouvernementale peut refuser de communiquer des renseignements personnels si leur communication risquerait vraisemblablement de nuire aux activités visant à faire respecter les lois—dans ce cas-ci, la *Loi sur le casier judiciaire*. La CLCC a aussi commencé à exiger des renseignements autres que le nom et la date de naissance pour valider l'identité d'un demandeur, notamment son numéro du Système d'empreintes digitales, le numéro de référence de la CLCC ou une copie de son casier judiciaire.

L'entreprise a déposé une plainte auprès du Commissariat, alléguant que la CLCC savait pertinemment que la plupart des demandeurs ne possédaient pas les renseignements personnels exigés pour valider leur identité car ils n'avaient jamais été déclarés coupables d'une infraction. Pour sa part, la CLCC a fait valoir plusieurs arguments pour justifier les mesures prises et sa prudence compte tenu de la sensibilité des renseignements en cause.

Après avoir analysé minutieusement la plainte, nous sommes d'accord avec le plaignant. À notre avis, l'alinéa 22(1)*b*) peut être invoqué uniquement pour refuser de communiquer de l'information concernant une suspension de casier judiciaire lorsque le demandeur et l'individu dont le casier a été suspendu pourraient être la même personne, mais qu'il n'est pas possible de le confirmer. La communication de ce type de renseignements sensibles alors que les exceptions prévues par la *Loi sur le casier judiciaire* ne s'appliquent pas peut constituer une infraction à la Loi. Cependant, la révélation du fait qu'aucun casier n'a été trouvé ne constitue pas selon nous une infraction à cette loi.

De plus, il ne nous semble pas raisonnable que la CLCC exige que tous les demandeurs lui fournissent des renseignements d'identification supplémentaires. Par contre, dans les rares cas où elle trouve de l'information pouvant correspondre à une demande à partir du nom et de la date de naissance du demandeur, il serait acceptable qu'elle tente de confirmer plus précisément l'identité du demandeur.

Nous avons conclu que les plaintes étaient fondées. La CLCC n'a pas accepté nos conclusions ni nos recommandations et refuse encore de répondre aux demandes présentées en vertu de la *Loi sur la protection des renseignements personnels* à moins que le demandeur ne fournisse des renseignements d'identification supplémentaires.

À la suite de notre enquête, le ministre de la Sécurité publique et de la Protection civile nous a envoyé une lettre dans laquelle il déclarait avoir demandé à ses fonctionnaires de concilier les dispositions de la *Loi sur le casier judiciaire* et de la *Loi sur la protection des renseignements personnels* ainsi que celles de leurs règlements d'application respectifs. Nous estimons qu'il n'y a pas d'incompatibilité entre les exigences imposées par les deux lois, comme nous l'avons indiqué dans notre rapport de conclusions sur le refus d'accès à la CLCC, mais nous sommes prêts à discuter de cette question avec des représentants de Sécurité publique Canada.

ENQUÊTES MENÉES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Le Commissariat à la protection de la vie privée du Canada surveille la conformité des institutions fédérales aux exigences de la *Loi sur la protection des renseignements personnels*. Il est tenu par la loi de faire enquête sur toutes les plaintes qu'il reçoit en vertu de cette loi.

En 2016-2017, le Commissariat a accepté 1 357 plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels.* Ce nombre ne tient pas compte des plaintes multiples concernant un seul incident ni des plaintes multiples déposées par un seul individu.

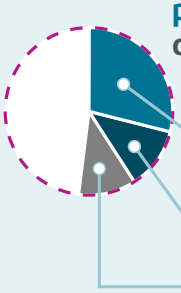
Si l'on exclut les plaintes multiples, le nombre de plaintes acceptées a légèrement diminué (2 %) comparativement à l'exercice précédent. Toutefois, par rapport à il y a cinq ans, le nombre de plaintes reçues par le Commissariat en vertu de la *Loi sur la protection des renseignements personnels* est passé de 1 114 en 2012-2013 à 1 357 en 2016-2017, soit une progression d'environ 22 %.

Le Commissariat a fermé 1 083 enquêtes en vertu de la *Loi sur la protection des renseignements personnels*. En 2016-2017, nos enquêtes ordinaires ont duré dix mois en moyenne, soit la même durée qu'au cours de l'exercice précédent. Cependant, la durée moyenne des enquêtes, tous types confondus (enquêtes ordinaires et dossiers fermés par règlement rapide), a légèrement augmenté cette année, passant de 6,7 à 7,4 mois. Le degré de complexité des plaintes augmente et, par conséquent, il en va de même pour la durée des enquêtes. En conséquence, le nombre de plaintes actives depuis plus de 12 mois continue d'augmenter.

ENQUÊTES MENÉES EN 2016–2017 – *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

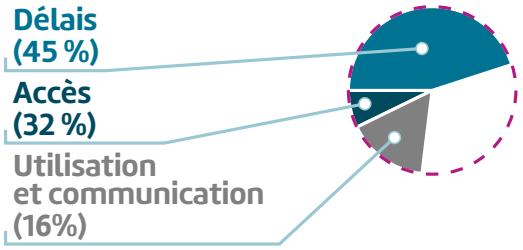
1 357 plaintes acceptées

Institutions visées
par le plus grand nombre de plaintes acceptées



- Service correctionnel du Canada (29%)
- Gendarmerie royale du Canada (12 %)
- Défense nationale (11 %)

Types de plaintes les plus courantes



- Délais (45 %)
- Accès (32 %)
- Utilisation et communication (16%)

Gestion du nombre de plaintes

Nous avons mis en œuvre notre stratégie de traitement des plaintes multiples pour éviter les situations qui pourraient avoir des répercussions disproportionnées sur les ressources allouées aux enquêtes, par exemple lorsqu'un même individu dépose plusieurs plaintes. Cette stratégie limite le nombre d'enquêtes ouvertes pour un individu en tout temps, ce qui nous permet de gérer la charge de travail et d'assurer une distribution équitable des ressources parmi les plaignants.

En outre, nous continuons d'avoir davantage recours à notre processus de règlement rapide lorsqu'il est approprié de le faire—près de 40 % des plaintes du secteur public ont été réglées à l'aide de cette approche en 2016-2017. Toutefois, le délai de traitement moyen des plaintes réglées rapidement s'est allongé, passant de 2,2 mois en 2015-2016 à 3,8 mois en 2016-2017.

Nous sommes constamment en quête de nouvelles façons d'optimiser les ressources limitées allouées aux enquêtes. Par exemple, au cours de l'exercice, nous avons mis en œuvre un nouveau cadre de gestion du risque à l'appui de nos efforts en vue de consacrer nos ressources aux plaintes ayant la plus grande incidence sur la vie privée. De plus, les mesures de modernisation de notre système de gestion des cas nous aideront à mieux dégager les tendances et à en rendre compte, ce qui favorisera les initiatives de sensibilisation des institutions afin qu'elles traitent de façon proactive les questions liées à la protection de la vie privée.

Résumé des conclusions d'enquêtes clés

La *Loi sur la protection des renseignements personnels* impose au commissaire à la protection de la vie privée du Canada des obligations strictes en matière de confidentialité. Le commissaire peut rendre publiques les conclusions des enquêtes menées en vertu de la Loi uniquement dans des rapports annuels ou des rapports spéciaux au Parlement.

Nous reconnaissons l'importance que revêt la confidentialité pour faciliter la fonction d'ombudsman du Commissariat, mais la communication des conclusions d'enquête est dans l'intérêt public dans certains cas—par exemple pour éclairer les débats parlementaires et les discussions publiques en temps opportun. Comme l'indiquent les résumés des conclusions d'enquête figurant dans la présente section, la communication publique des « leçons apprises » dans certains cas précis permet aussi parfois d'encourager les institutions fédérales à adopter des mesures proactives pour éviter les plaintes semblables à l'avenir.

Dans son rapport concernant l'examen de *Loi sur la protection des renseignements personnels*, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique s'est dit d'accord avec notre recommandation visant à modifier la Loi de façon à conférer au commissaire le pouvoir discrétionnaire de communiquer les conclusions d'une enquête lorsqu'il juge que c'est dans l'intérêt public plutôt que d'attendre à la fin de l'exercice en question (voir la section sur la Réforme de la *Loi sur la protection des renseignements personnels*).

Nous espérons que cet aspect de la loi pourra être modifié, mais nous continuerons de faire état des enquêtes clés dans nos rapports au Parlement. Nous présentons ci-après quelques dossiers importants sur lesquels nous avons fait enquête au cours de l'exercice.

Bureau du Conseil privé—Site Web MaDemocratie.ca

Le Bureau du Conseil privé (BCP) a lancé le site Web MaDemocratie.ca au début de décembre 2016 dans le cadre d'un dialogue national sur la réforme électorale. On y invitait les participants à répondre à un sondage et à exprimer leur opinion sur différentes questions concernant la réforme électorale, en promettant de préserver l'anonymat des réponses individuelles. Une fois le questionnaire rempli, les résultats étaient affichés à l'intention des participants sous forme de profil de groupe d'électeurs ou « profil-type » (défenseurs, critiques, pragmatiques, coopérateurs ou innovateurs). Le site Web invitait les participants à partager leurs résultats avec leurs amis sur les médias sociaux.

Dans une plainte adressée au Commissariat, le plaignant alléguait que le site Web promettait de préserver l'anonymat, mais qu'il avait recours au module de suivi Facebook (Facebook Connect). Selon

lui, le gouvernement pouvait avoir utilisé la fonction de suivi même s'il affirmait publiquement aux citoyens que leur anonymat serait préservé.

Notre enquête a confirmé que le site Web MaDemocratie.ca était conçu de façon à permettre l'intervention d'un tiers, y compris Facebook (dans le contexte de notre enquête, un « tiers » est une autre organisation qui contribue au contenu d'un site Web, qui en facilite l'accès ou qui ajoute du contenu). Le module Facebook Connect a été installé sur le site Web pour partager des résultats (bouton de partage de Facebook).

Dans le cadre de notre enquête, nous n'avons trouvé aucune preuve indiquant que le BCP avait recours à des mesures pour identifier les participants au sondage ou pour connaître les réponses individuelles aux questions du sondage. Par contre, il n'a pas été démontré que le site MaDemocratie.ca avait été conçu dans un souci de protection de la vie privée.

Notre examen a confirmé que la conception du site Web permettait l'intervention d'un tiers et que les adresses IP et d'autres renseignements de navigation sur Internet étaient communiqués à ce tiers dès que la page d'accueil du site MaDemocratie.ca était chargée, et ce, sans que l'utilisateur autorise ou active délibérément le partage sur les réseaux sociaux. Nous sommes arrivés à la conclusion que, dans certains cas, cette information aurait pu être associée à certaines personnes, ce qui aurait constitué une communication de leurs renseignements personnels et ainsi accru le risque que leurs activités sur le site n'aient pas été véritablement anonymes. On ne nous a pas démontré que le BCP avait obtenu le consentement requis pour communiquer ces renseignements personnels et nous avons estimé que la plainte était fondée.

Combinée avec d'autres renseignements, une adresse IP peut permettre de dresser un profil exhaustif d'une personne identifiable et révéler de façon assez juste les activités de cette personne sur Internet, comme en témoignent les recherches. En vertu de la politique du gouvernement, les adresses IP sont considérées comme des renseignements personnels.

Notre analyse technique a révélé qu'une conception différente du site Web aurait pu permettre d'éviter l'échange prématuré de renseignements en restreignant le chargement des éléments de tiers aux seuls cas où ils étaient nécessaires (c.-à-d. lorsqu'un utilisateur autorise ou active délibérément le partage sur les réseaux sociaux). Nous avons constaté que ces renseignements étaient communiqués avant même que la personne puisse prendre connaissance des pratiques du site Web et décider en toute connaissance de cause si elle souhaitait ou non interagir sur le site.

Nous reconnaissons que le gouvernement du Canada doit suivre le rythme des technologies modernes et des outils de communication offerts en ligne et les adopter. Les médias sociaux représentent l'un de ces outils, puisqu'ils offrent une plus grande connectivité et la possibilité de se servir des interactions sociales pour entrer en contact avec les Canadiens. L'initiative MaDémocratie était une plateforme novatrice dont le but consistait à recueillir l'opinion et le point de vue des Canadiens. Toutefois, le BCP aurait dû faire preuve d'une plus grande prudence dans son évaluation de l'initiative afin de recenser les risques d'atteinte à la vie privée que posait le site et de les atténuer avant son lancement, d'autant plus que le site promettait de préserver l'anonymat.

Nous avons formulé plusieurs recommandations au BCP pour veiller à ce que la protection de la vie privée soit considérée comme un élément central de la conception initiale et de l'administration de toute initiative similaire. Nous sommes heureux de constater que le BCP a reconnu que les problèmes que nous avions soulevés constituent un rappel utile de la nécessité de comprendre les outils en ligne de manière à ce que la protection de la vie privée des personnes demeure une priorité importante. En outre, nous nous réjouissons que le BCP est déterminé à

protéger les renseignements personnels des Canadiens tout en veillant à ce que ses politiques soient adaptées aux nouvelles technologies et qu'elles soutiennent efficacement les efforts déployés par le gouvernement pour mobiliser les Canadiens de façon novatrice. Le BCP s'est par ailleurs engagé à l'avenir à mener des évaluations des facteurs relatifs à la vie privée (EFVP) au sujet de la conception d'un nouveau projet et de ses répercussions sur la protection des renseignements personnels.

Pour en savoir plus, consultez la version intégrale du rapport sur les conclusions de notre enquête au sujet de MaDemocracie.ca.

Santé Canada—Collecte de renseignements personnels pour les services de santé non assurés

Dans la plainte qu'il a déposée au nom de plus de 20 médecins desservant des communautés des Premières Nations et des communautés inuites, un député alléguait que Santé Canada exigeait plus de renseignements personnels que nécessaire pour traiter les demandes de paiement relatifs au Programme des services de santé non assurés (SSNA).

Le Programme des SSNA fournit aux membres admissibles des Premières Nations et aux Inuits reconnus une couverture en matière de services de santé non couverts par d'autres régimes ou programmes. À l'issue d'une enquête, nous avons conclu que cette plainte était fondée. Les renseignements détaillés relatifs au diagnostic recueillis par Santé Canada allaient au-delà de ce qui était nécessaire pour traiter les demandes de remboursement, ce qui portait atteinte à la vie privée des patients Inuits et membres des Premières Nations, d'autant plus qu'il s'agit de renseignements personnels sensibles sur la santé.

Au cours de notre enquête, Santé Canada a accepté de modifier le formulaire de traitement des demandes en supprimant la section à l'origine de la collecte excessive de renseignements personnels.

Pour en savoir plus, consultez la version intégrale du rapport sur les conclusions de l'enquête sur le Programme des SSNA.

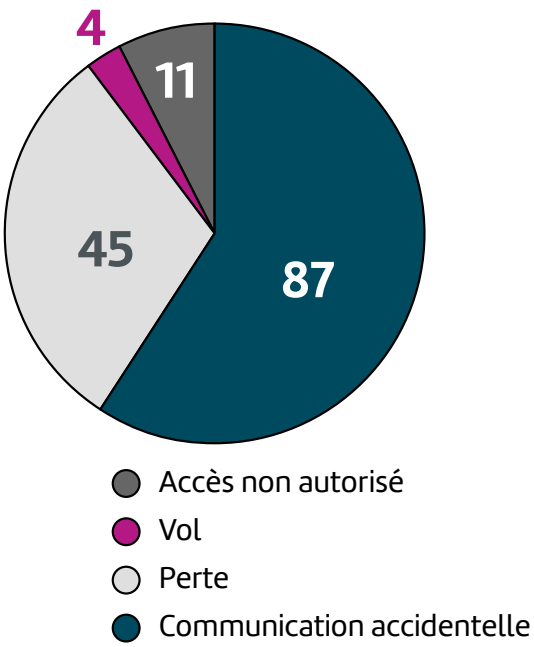
Atteintes à la vie privée

Selon la politique du Secrétariat du Conseil du Trésor, les institutions fédérales sont tenues de déclarer au Commissariat toute atteinte substantielle à la vie privée[10]. Lorsqu'il examine ce type d'incident, le Commissariat se penche sur les circonstances qui ont mené à l'atteinte—afin de déterminer s'il s'agit d'un problème systémique—ainsi que sur les mesures que peut avoir prises l'institution pour atténuer le risque. À la lumière de nos constatations, nous recommandons parfois des mesures correctives pour aider à éviter que des situations semblables se reproduisent.

Toutefois, les institutions ne se conforment pas toutes systématiquement à la politique du Conseil du Trésor. Nous avons recommandé de modifier la *Loi sur la protection des renseignements personnels* pour obliger expressément les institutions fédérales à déclarer au Commissariat les atteintes substantielles à la vie privée. Ainsi, le Commissariat aurait une meilleure idée de l'ampleur du problème dans l'ensemble du gouvernement fédéral, il serait consulté dans la démarche visant à réagir à l'atteinte et à atténuer ses répercussions sur les individus et il pourrait informer les institutions des mesures à leur disposition pour réduire le risque d'atteintes ultérieures.

Les statistiques qui suivent illustrent l'incohérence dans la déclaration des atteintes. Après une augmentation annuelle stable des déclarations depuis que le Commissariat a commencé à faire le suivi des atteintes à la sécurité des données dans le secteur public, seulement 27 institutions fédérales sur plus de 250 institutions assujetties à la Loi ont informé officiellement le Commissariat de 147 atteintes en

10 Une atteinte substantielle à la vie privée présente le risque d'incidence le plus élevé. Par définition, elle porte sur des renseignements personnels sensibles et on pourrait raisonnablement s'attendre à ce qu'elle cause un préjudice ou un dommage sérieux à l'intéressé ou qu'elle touche un grand nombre d'individus.



TYPES D'ATTEINTES DÉCLARÉES

2016-2017, soit moins de la moitié par rapport à l'exercice précédent. Cette baisse était généralisée, à une exception près : Emploi et Développement social Canada a déclaré un nombre beaucoup plus élevé d'atteintes à la vie privée. Toutefois, comme au cours des exercices antérieurs, quelques institutions ont déclaré près des deux tiers des incidents l'an dernier. Voir l'annexe 2, « Tableaux statistiques—Atteintes en vertu de la *Loi sur la protection des renseignements personnels,* par institution ».

Comme ce fut le cas au cours des exercices antérieurs, les institutions ont déclaré un nombre apparemment négligeable de cyberincidents. En fait, un seul incident de piratage sur le Web a été déclaré en 2016-2017. Lors des exercices précédents, par exemple en 2014-2015, le Commissariat avait reçu seulement deux avis de cyberatteintes, soit une intrusion dans le réseau du Conseil national de recherches du Canada et une liée à la faille de sécurité *Heartbleed*. Une seule institution, soit l'ARC, a déclaré le tristement célèbre incident *Heartbleed*.

Le Commissariat a soulevé la question avec le Secrétariat du Conseil du Trésor et encouragé le milieu fédéral de l'accès à l'information et de la protection des renseignements personnels à inciter activement les agents de sécurité et les dirigeants principaux de l'information des ministères à se familiariser avec les incidents de cybersécurité.

Rien n'explique clairement la diminution considérable du nombre de déclarations d'atteintes à la sécurité des données au cours de l'exercice. Nous ferons un suivi auprès des institutions dans les prochains mois pour mieux comprendre cette baisse.

Résumé des atteintes clés

Système de paye Phénix

Services publics et Approvisionnement Canada (SPAC) administre la paye de quelque 290 000 fonctionnaires travaillant dans 101 institutions fédérales, ce qui en fait l'un des plus grands fournisseurs de services de paye au pays. Il a déployé au début de 2016 le système de paye Phénix, une application développée par IBM. En 2016-2017, SPAC a avisé le Commissariat d'atteintes à la vie privée liées au système Phénix.

À cet instant, le Commissariat avait été informé que ces incidents impliquaient un nombre limité d'institutions et ne portaient que sur le nom des employés et les codes d'identification de dossier personnel (CIDP), et les renseignements n'avaient été communiqués qu'à un nombre limité de fonctionnaires fédéraux. SPAC a soutenu qu'à son avis, le risque pesant sur les personnes touchées était « très faible ».

Après la déclaration des atteintes à la vie privée, nous avons reçu trois plaintes s'y rapportant. Selon les plaignants, ces atteintes avaient une portée beaucoup plus large que ne l'avait indiqué SPAC et le ministère était au courant d'un problème potentiel lié à la protection de la vie privée bien avant le déploiement du système Phénix. Au cours de la phase initiale de notre enquête, SPAC a réitéré dans ses premières observations que les incidents impliquaient un nombre limité d'institutions et ne portaient que sur le nom des employés et les CIDP et que les

renseignements n'avaient été communiqués qu'à un nombre limité de fonctionnaires fédéraux. Cependant, l'institution nous a informés que, pour au moins deux cas, les problèmes ayant mené aux atteintes à la vie privée n'avaient pas été résolus. Dans le cadre de notre enquête, nous avons établi qu'au moins 11 cas d'atteinte à la vie privée s'étaient produits et que les renseignements en cause incluaient le nom des employés, leur CIDP et l'information sur leur salaire. La majorité des vulnérabilités étudiées avait une portée pangouvernementale, ce qui signifie que l'information de l'ensemble des employés inscrits au système de paye Phénix au moment de chacun des incidents était à risque. Nous avons établi que dans certains des cas d'atteinte à la vie privée, des renseignements pouvaient être modifiés et des opérations pouvaient être effectuées. De plus, nous avons déterminé que certaines vulnérabilités demeurent et que celles-ci pourraient mener à d'autres incidents.

Dans ce dossier, il est particulièrement troublant que SPAC ne soit pas en mesure de surveiller ou de vérifier qui a accès aux renseignements personnels contenus dans Phénix—fonctionnalité que le Conseil du Trésor recommande d'intégrer dans les nouveaux systèmes de TI. Selon les fonctionnaires de SPAC, une telle fonctionnalité aurait un effet important sur le rendement de Phénix. Ils ont toutefois précisé qu'ils pouvaient vérifier les opérations effectuées dans le système. Même si nous n'avons relevé aucune preuve que les renseignements personnels en cause ont été communiqués à des personnes à l'extérieur du gouvernement, nous avons observé dans d'autres circonstances des cas d'employés d'autres ministères ainsi que de SPAC fouillant les données sans autorisation. Par exemple, en avril 2017, SPAC nous a signalé un autre cas d'atteinte à la vie privée qui impliquait un employé contractuel, lequel utilisait Phénix pour fouiner les données des membres de sa famille employés de la fonction publique fédérale. De manière générale, le vol d'identité et la fraude financière sont des préjudices potentiels qui peuvent découler d'une communication non autorisée de renseignements personnels.

Notre enquête a déterminé que les atteintes à la vie privée étaient le résultat d'une combinaison de tests inadéquats, d'erreurs de codage et d'une insuffisance au chapitre des mécanismes de surveillance et de contrôle du système Phénix. Nous avons conclu que les plaintes étaient fondées. Nous avons formulé plusieurs recommandations pour aider SPAC à résoudre les problèmes qui ont contribué aux incidents, entre autres de mettre au point et de mettre en place des mécanismes de contrôle pour surveiller et consigner l'accès aux renseignements personnels contenus dans le système.

L'institution a accepté la plupart de nos recommandations. En ce qui concerne la recommandation susmentionnée, SPAC a déclaré qu'il avait à cœur de trouver une solution pratique. Nous lui avons demandé de faire un suivi auprès du Commissariat après six mois afin de rendre compte des progrès réalisés dans la mise en œuvre de nos recommandations. Pour de plus amples renseignements, consulter le rapport intégral sur notre enquête portant sur le Système de paye Phénix.

Communication par courriel de renseignements personnels d'employés de Services publics et Approvisionnement Canada

En plus des atteintes à la vie privée liées au système Phénix, en septembre 2016, SPAC nous a fait part d'une autre atteinte à la vie privée de fonctionnaires. L'institution a déclaré qu'un agent des ressources humaines avait fait parvenir à 180 cadres supérieurs de SPAC un courriel auquel était jointe une feuille de calcul Excel contenant les renseignements personnels de leurs employés servant à la planification des ressources humaines. La pièce jointe contenait aussi malencontreusement un onglet dans lequel figuraient les renseignements des 14 241 employés de SPAC, entre autres leur nom, leur âge, leur sexe, leur salaire ainsi que des renseignements sur leur régime de retraite et leur situation en regard de l'équité en matière d'emploi. Le Commissariat a reçu par la suite plusieurs plaintes de personnes touchées. Nous avons souligné dans notre suivi que SPAC avait pris

des mesures pour maîtriser la situation, notamment une mesure corrective essentielle, soit une commande de recherche et de suppression permettant au personnel de Services partagés Canada de supprimer automatiquement le courriel et la pièce jointe de tous les comptes de SPAC. Les plaintes ont été fermées en octobre 2016 par règlement rapide à la satisfaction des plaignants.

Communication accidentelle de renseignements personnels sur la santé par Anciens Combattants Canada

En janvier 2017, Anciens Combattants Canada (ACC) a déclaré qu'une lettre envoyée à environ 3 300 vétérans par la Croix Bleue Medavie avait été postée dans une enveloppe à fenêtre à travers laquelle on pouvait lire : « Objet : Cannabis à des fins médicales—Renseignements sur la nouvelle politique de remboursement ». Le Commissariat a reçu de nombreuses plaintes des personnes touchées et a ouvert une enquête à ce sujet.

Perte par l'Agence du revenu du Canada d'un DVD contenant des données chiffrées

Également en janvier 2017, l'Agence du revenu du Canada (ARC) a avisé le Commissariat qu'un DVD contenant les renseignements fiscaux de 28 000 résidents du Yukon, envoyé par courrier recommandé au gouvernement du territoire, n'était jamais parvenu à destination. Il est inquiétant que les données sensibles d'un si grand nombre de Canadiens puissent être mises en péril en raison d'une erreur dans le processus d'expédition, mais nous étions heureux d'apprendre que le DVD était protégé par un mot de passe et que les renseignements étaient chiffrés à un niveau de sécurité très élevé—deux recommandations du Commissariat relatives aux dispositifs de stockage portatifs (voir nos Conseils à l'intention des institutions fédérales sur l'utilisation des dispositifs de stockage portatifs). Nous estimons donc que l'ARC a pris les mesures appropriées pour protéger les renseignements et nous sommes d'accord avec l'Agence sur le fait qu'il serait très peu probable que les renseignements des contribuables soient mis en péril, même si une personne non autorisée obtenait le DVD.

Passeports

Le Commissariat a reçu un avis l'informant d'un grand nombre d'atteintes à la vie privée ainsi que quelques plaintes liées à la perte ou à la communication non autorisée de données de passeport. Près de la moitié des 45 incidents de cette nature déclarés en 2016-2017 concernaient la perte de passeports.

La nécessité de préciser les compétences a compliqué l'examen de ces incidents : Passeport Canada a cessé d'exister en 2013 et le programme de passeports a été transféré à Immigration, Réfugiés et Citoyenneté Canada. Service Canada, qui relève d'Emploi et Développement social Canada (EDSC), assume la responsabilité de certaines opérations liées aux passeports, entre autres la gestion du réseau des bureaux des passeports. De plus, la distribution des passeports par la Société canadienne des postes (SCP) est assujettie à un protocole d'entente entre la SCP et IRCC. Affaires mondiales Canada a aussi déclaré quelques atteintes à la vie privée mettant en cause la perte de passeports pendant leur transfert vers une mission canadienne (consulats et ambassades) ou entre deux missions à l'étranger.

VÉRIFICATIONS ET EXAMENS

La *Loi sur la protection des renseignements personnels* et la LPRPDE confèrent au Commissariat le pouvoir de vérifier les pratiques des institutions fédérales et des organisations du secteur privé en matière de protection des renseignements personnels—toutefois, en vertu de la LPRPDE, le Commissariat ne peut procéder à la vérification d'une organisation du secteur privé à moins d'avoir des motifs de croire qu'elle a enfreint une disposition de la Loi ou qu'elle ne respecte pas une recommandation énoncée à l'annexe 1.

Le Commissariat a le pouvoir de procéder à des vérifications pour s'assurer qu'une organisation gère ses fonds de renseignements personnels conformément aux obligations qui lui incombent en vertu de la loi. Il s'agit de l'un des moyens qu'il prend pour s'acquitter de sa mission consistant à protéger et à promouvoir le droit à la vie privée. Les vérifications peuvent porter, entre autres, sur les mesures de contrôle matérielles et les mesures de sécurité utilisées pour protéger les renseignements personnels détenus par l'organisation, sur les politiques, procédures et pratiques en place et sur la façon dont l'organisation gère les incidents d'atteinte à la vie privée. De cette façon, le Commissariat est en mesure de déterminer de manière proactive les aspects à améliorer et de mettre en évidence les pratiques exemplaires en matière de protection de la vie privée.

Une grande partie de nos activités de vérification en 2016-2017 était dictée par notre préoccupation constante concernant les répercussions, sur la vie privée, des lois et des programmes récemment adoptés en matière de sécurité nationale—dans le cadre de ces initiatives, les institutions fédérales sont souvent autorisées à recueillir et à communiquer de grandes quantités de renseignements personnels en étant soumises à une surveillance et à des obligations de transparence et de reddition de comptes limitées, voire inexistantes.

Centre d'analyse des opérations et déclarations financières

Outre les vérifications concernant la sécurité nationale présentées à la page 63, le Commissariat a procédé à son troisième examen des pratiques du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) en matière de protection de la vie privée.

CANAFE a été créé en 2001 par la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, en vertu de laquelle les personnes et les entités de divers secteurs doivent examiner de près les transactions financières des clients et en rendre compte. Ces entités, dont le nombre pourrait atteindre 300 000, transmettent à CANAFE des rapports contenant des renseignements personnels sensibles concernant des Canadiens. Certains rapports sont transmis à l'insu des intéressés, les entités déclarantes n'ont pas à obtenir leur consentement pour transmettre les rapports et il est possible que les intéressés ne puissent pas avoir accès aux renseignements.

L'obligation de protéger les fonds de renseignements, bien qu'elle s'applique à tous les ministères, est accentuée pour des organismes tels que CANAFE. Les renseignements personnels recueillis par CANAFE sont à la fois très sensibles et détaillés : on estime que les bases de données du Centre comptaient en 2012 environ 165 millions de rapports contenant des renseignements personnels. C'est pourquoi la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* exige que le Commissariat examine régulièrement les mesures prises par CANAFE pour protéger les renseignements qu'il reçoit ou qu'il recueille en application de la Loi. Nous avons procédé à une vérification de CANAFE à deux reprises par le passé, soit en 2009 et en 2013. Nous avons alors soulevé plusieurs préoccupations et formulé des recommandations.

Vérification de CANAFE

Nous avons effectué une troisième vérification de CANAFE au cours de l'exercice. Nous nous sommes alors concentrés sur la structure technique qui soutient ses données et sur le rôle de Services partagés Canada (SPC) dans la protection de l'infrastructure de TI où sont stockés les renseignements de l'organisme. Nous avons aussi examiné les progrès réalisés par CANAFE dans sa réponse aux recommandations formulées à l'issue de notre vérification de 2013.

Au cours des vérifications précédentes, nous avons constaté que CANAFE recevait et conservait de l'information au-delà de ce qui est autorisé par la loi et qu'il devait améliorer le contrôle initial et la surveillance continue des déclarations pour s'assurer que ses fonds de renseignements sont pertinents sans être excessifs. Dans le cadre de la troisième vérification, tout en reconnaissant les efforts déployés par CANAFE pour améliorer ses pratiques de protection des renseignements personnels, nous avons remarqué qu'il avait peu progressé dans la mise en œuvre des recommandations formulées en 2013, particulièrement pour limiter la réception, la collecte et la conservation des renseignements personnels à ceux qui sont directement liés à l'exécution de son mandat. Nous avions recommandé à CANAFE de poursuivre ses efforts pour mettre en œuvre des mesures de contrôle initial rigoureuses et exhaustives afin de s'assurer que les dossiers et les rapports qu'il conserve dans sa base de données respectent les seuils de déclaration prévus par la loi et qu'ils ne renferment pas de renseignements personnels non nécessaires ou en quantité excessive. Nous lui avions aussi recommandé d'éliminer les rapports jugés non conformes au seuil de déclaration établi.

De même, nous avons remarqué que, dans le cadre de ses activités visant à vérifier si les entités déclarantes respectent les obligations qui leur incombent en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes,* CANAFE avait recueilli des renseignements sensibles non liés à ses activités de conformité, par exemple des données sur les employés des entités déclarantes. Cette pratique va à l'encontre des politiques internes de CANAFE et des politiques applicables du Secrétariat du Conseil du Trésor du Canada. Nous avons recommandé à CANAFE d'entreprendre un exercice interne de réduction au minimum et d'élimination des données afin de détruire les renseignements personnels qui se trouvent dans ses dossiers d'examen de la conformité et qui ne sont pas nécessaires dans le cadre de son travail à cet égard. Nous lui avons aussi recommandé d'augmenter ses efforts de sensibilisation pour aborder précisément la question des renseignements personnels inutiles fournis par les entités pendant les examens de la conformité.

Notre troisième vérification a mis au jour plusieurs problèmes de protection des renseignements personnels, entre autres l'absence d'une entente formelle entre CANAFE et SPC définissant clairement leurs responsabilités et leurs rôles respectifs afin d'assurer la sécurité de l'infrastructure de TI. L'entente opérationnelle actuelle entre les deux institutions ne prévoit aucune exigence en matière de sécurité et de protection des renseignements personnels pour protéger les fonds de renseignements de CANAFE. En l'absence d'une définition claire des rôles et des responsabilités, il y a un risque de consultation, d'utilisation ou de communication inappropriées des renseignements personnels. Nous avons donc recommandé à CANAFE de collaborer avec SPC pour mettre en place une entente qui définit clairement les rôles et les responsabilités en matière de sécurité de la TI et les clauses pertinentes liées à la protection de la vie privée et à la sécurité.

Dans cette vérification, nous avons remarqué que SPC n'avait effectué aucune évaluation de la sécurité et d'autorisation (ESA) sur l'infrastructure à l'appui des systèmes de CANAFE depuis son transfert vers SPC en 2012. Nous avons constaté que CANAFE avait lui-même mis à jour les évaluations de sécurité antérieures pour ses systèmes, sans la participation de la direction de SPC. Les activités d'ESA sont des processus formels et permanents conçus pour s'assurer que les systèmes ou les services font l'objet d'examens de sécurité et que les lacunes détectées ont été

corrigées. Sans une évaluation des risques d'atteinte à la vie privée au moyen de ces processus, il est possible que des risques d'atteinte à la vie privée et à la sécurité des renseignements personnels de CANAFE ne soient pas repérés ni atténués. Nous avons recommandé à CANAFE de présenter une demande officielle à SPC pour lancer le processus d'ESA afin de s'assurer que l'infrastructure de TI de SPC où sont hébergées les données de CANAFE est certifiée et accréditée.

Les entités doivent déclarer à CANAFE et à l'ARC les télévirements de 10 000 $ ou plus. Du point de vue fonctionnel, les déclarations sont transmises à l'ARC par l'intermédiaire d'un système de SPC qui ne procède pas à des ESA. Sans une autorisation formelle de la part de la direction pour l'exploitation de ce service, rien ne garantit que les exigences en matière de sécurité pour le service sont respectées ni que les mesures de contrôle et de protection fonctionnent comme prévu. Cette responsabilité incombe exclusivement à SPC. Toutefois, comme CANAFE doit utiliser ce système, nous lui avons recommandé de présenter une demande officielle à SPC pour lancer le processus d'ESA afin de s'assurer que l'infrastructure de TI de SPC où passent les données de CANAFE est certifiée et accréditée.

CANAFE a accepté toutes nos recommandations. On trouvera la réponse détaillée de l'organisation dans le rapport de vérification de CANAFE.

ÉVALUATIONS DES FACTEURS RELATIFS À LA VIE PRIVÉE

Une approche proactive est essentielle à la protection de la vie privée—et l'évaluation des facteurs relatifs à la vie privée (EFVP) est l'un des principaux outils de prévention permettant de cerner et d'atténuer les risques d'atteinte à la vie privée qui peuvent être associés aux nouveaux programmes ou services gouvernementaux. Selon la politique gouvernementale, pratiquement toutes les institutions fédérales doivent effectuer une EFVP avant de mettre en œuvre un programme ou un service nouveau ou modifié susceptible d'avoir une incidence sur la vie privée. Les institutions doivent faire parvenir les EFVP au Commissariat, qui les examinera et pourrait formuler des recommandations pour régler les problèmes relevés sur le plan de la protection de la vie privée.

Les EFVP permettent aux institutions gouvernementales de rendre des comptes à l'égard de la protection des renseignements personnels des Canadiens. Elles les aident à cerner les risques d'atteinte à la vie privée, à en évaluer l'incidence et à les gérer en mettant en œuvre des mesures d'atténuation appropriées.

À mesure que les ministères déploient de nouvelles technologies et techniques qui leur permettent de recueillir une quantité et une variété sans cesse croissantes de renseignements personnels, il est de plus en plus nécessaire d'effectuer des EFVP exhaustives pour atténuer les risques.

D'après la *Politique sur la protection de la vie privée* du SCT, les institutions gouvernementales doivent aviser le commissaire à la protection de la vie privée de toute initiative prévue (loi, règlement, politique, programme) pouvant avoir un rapport avec la Loi ou l'une de ses dispositions ou pouvant avoir une incidence sur la vie privée des Canadiens. Selon la politique, cet avis doit être transmis suffisamment tôt pour permettre au commissaire d'examiner les enjeux et d'en discuter. De plus, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* insiste sur le rôle essentiel des EFVP pour s'assurer que les répercussions sur la vie privée sont réglées *avant* la mise en œuvre d'un programme ou d'une activité comportant des renseignements personnels.

Certaines institutions fédérales font l'effort de consulter le Commissariat avant de mettre en œuvre des programmes ou des activités susceptibles de porter atteinte à la vie privée. Elles présentent leurs EFVP suffisamment tôt pour recevoir des conseils utiles et prendre les mesures nécessaires. Cependant, il arrive souvent que nous ne soyons pas consultés et même qu'aucune EFVP ne soit effectuée. Nous savons entre autres que certaines institutions utilisent des renseignements personnels sensibles pour administrer des programmes et des activités susceptibles de porter atteinte la vie privée. C'est regrettable.

Il est également regrettable que même si les institutions présentent au Commissariat les EFVP exigées, elles le font souvent très peu de temps avant et parfois même après la mise en œuvre d'un programme. Lorsqu'il reçoit une EFVP suffisamment tôt, le Commissariat est en mesure de mener un examen plus approfondi et de formuler des conseils, des commentaires et des recommandations ainsi que d'offrir des consultations *avant* la mise en œuvre du programme. On réduit alors considérablement le risque de devoir envisager de mettre fin à des programmes ou à des services ou de les modifier après leur mise en œuvre dans le but de respecter les exigences en matière de protection de la vie privée. Les exemples cités dans la présente section

illustrent comment le Commissariat peut, en se fondant sur l'examen des EFVP, recommander des mesures souvent toutes simples que les ministères peuvent prendre afin d'éliminer ou d'atténuer les risques d'atteinte à la vie privée—et les risques qui se posent lorsque les institutions ne présentent pas les EFVP à temps pour que le Commissariat puisse les examiner adéquatement ou qu'elles ne suivent pas les recommandations du Commissariat.

Les EFVP peuvent jouer un rôle essentiel dans la protection de la vie privée. C'est pourquoi, au lieu de s'en remettre à une simple politique, nous estimons qu'il faudrait obliger par voie législative les institutions fédérales à effectuer une EFVP pour les programmes nouveaux ou ayant subi des modifications importantes et à la transmettre au Commissariat avant la mise en œuvre de ces programmes. Nous avons recommandé de modifier en conséquence la *Loi sur la protection des renseignements personnels*.

Les EFVP en 2016–2017

En 2016-2017, 31 institutions fédérales ont déposé auprès du Commissariat 95 EFVP. Le Commissariat examine toutes les EFVP, mais ne formule pas de commentaires détaillés sur chacune d'elles. Une fonction de tri nous permet de canaliser nos ressources vers les initiatives les plus susceptibles de porter atteinte à la vie privée. Après les examens des EFVP, nous avons envoyé 22 lettres de recommandation qui donnaient des orientations et des conseils détaillés pour éliminer, réduire ou atténuer les risques d'atteinte à la vie privée liés à des initiatives particulières. De plus, avant même de procéder à une EFVP, plusieurs ministères fédéraux ont communiqué avec le Commissariat pour obtenir des conseils ou des orientations concernant un total de 18 initiatives pouvant porter atteinte à la vie privée.

Statistique Canada—Enquête canadienne sur les mesures de la santé

L'Enquête canadienne sur les mesures de la santé (ECMS) est menée par Statistique Canada en partenariat avec Santé Canada et l'Agence de la santé publique du Canada. Dans le cadre de cette enquête, Statistique Canada recueille auprès des Canadiens qui acceptent d'y participer des renseignements sur leur santé générale ainsi que des échantillons de sang et d'urine. Après avoir examiné l'EFVP portant sur l'enquête, le Commissariat a recommandé plusieurs mesures pour gérer les risques d'atteinte à la vie privée que posent ces renseignements personnels très sensibles.

En réponse à ces recommandations, Statistique Canada a apporté plusieurs améliorations afin de mieux protéger la vie privée des participants à l'enquête. L'organisme a notamment créé une vaste structure de gouvernance pour la Biobanque (où sont conservés les échantillons). La Biobanque fait maintenant l'objet d'une supervision permanente assurée par trois groupes tiers indépendants. En outre, des employés de l'ECMS se rendent sur place chaque année pour vérifier les procédures de laboratoire et les installations de stockage de la Biobanque.

Statistique Canada a aussi actualisé le site Web de la Biobanque en mettant plus en évidence le lien qui mène à la marche à suivre par les participants qui souhaitent se retirer de la Biobanque. Parmi les autres modifications apportées, mentionnons la révision du livret sur le consentement, auquel l'organisme a ajouté de l'information sur le retrait d'échantillon, et l'interdiction d'un accès direct des chercheurs tiers aux identificateurs personnels et aux échantillons biologiques.

Bureau du Conseil privé—Processus de nomination des membres du Conseil jeunesse du premier ministre

Le Conseil jeunesse du premier ministre, comité consultatif qui appuie le premier ministre dans son rôle de ministre de la Jeunesse, a lancé un appel de candidatures en juillet 2016. Les jeunes intéressés ayant entre 16 et 24 ans devaient fournir des renseignements biographiques, leurs coordonnées ainsi que des renseignements sur leurs études et leur expérience de travail. Le processus d'application impliquait le partage de leur expérience personnelle. On leur demandait de raconter en détails, par exemple, leur parcours d'immigration ou de parler

de leur santé physique et mentale ou encore de problèmes de dépendance ou de démêlés avec la justice. Le processus de candidature prévoyait aussi la participation de plusieurs fournisseurs tiers.

En réponse aux recommandations formulées par le Commissariat, le Bureau du Conseil privé (BCP) a cessé d'utiliser des champs de texte libre à la première étape du processus de candidature en ligne afin d'éviter de recueillir des renseignements personnels sensibles. Le BCP a aussi révisé l'avis de confidentialité affiché sur le site Web afin d'expliquer clairement aux candidats éventuels l'incidence sur la vie privée du stockage de leurs renseignements personnels sur les serveurs des entreprises privées dont le Bureau avait retenu les services pour gérer le processus de candidature.

En se fondant sur notre examen de l'EFVP, le BCP a aussi modifié son EFVP pour expliquer en détail les mesures de sécurité et les périodes de conservation qui visent à protéger les renseignements personnels recueillis dans le cadre du processus de candidature. Il ne demande plus de renseignements personnels détaillés aux candidats de la liste d'attente, à moins qu'ils n'aient été sélectionnés pour une évaluation approfondie. Le BCP a aussi précisé que les renseignements contenus dans les dossiers de candidature conservés sur des serveurs privés seront isolés et que seul le personnel autorisé y aura accès. Il a mis à jour ses ententes avec les entrepreneurs du secteur privé afin d'y prévoir des mesures de protection de la vie privée, notamment la confirmation écrite que les renseignements personnels recueillis par les entrepreneurs sont supprimés lorsqu'ils ne sont plus nécessaires pour les fins auxquelles ils ont été recueillis.

Immigration, Réfugiés et Citoyenneté Canada—Échange d'information avec le Royaume-Uni

Depuis 2000, le Home Office du Royaume-Uni et Immigration, Réfugiés et Citoyenneté Canada (IRCC) échangent de l'information de façon ponctuelle en vertu d'un protocole d'entente aux fins de l'administration et de l'application de leurs lois respectives régissant l'immigration, la citoyenneté, les systèmes de réinstallation de réfugiés et d'octroi d'asile. En septembre 2015, IRCC a mis à jour l'entente et y a ajouté l'ASFC à titre de participant, ce qui a nécessité une EFVP.

En réponse aux recommandations formulées par le Commissariat à l'issue de l'examen de l'EFVP portant sur le protocole d'entente, IRCC a demandé à son personnel de réduire le plus possible la quantité de renseignements personnels communiqués au cours des échanges et a exigé que toute communication d'information soit justifiée par écrit. Le ministère a aussi indiqué que des annexes de l'entente énuméreraient clairement les renseignements personnels pouvant être communiqués et recueillis et que l'on mettrait à jour les instructions sur l'exécution des programmes pour y inclure des procédures détaillées de collecte et d'élimination de renseignements.

GRC—Centre antifraude du Canada

Le Centre antifraude du Canada est le dépôt central des données sur les plaintes pour fraude à l'échelle nationale. Il recueille, stocke, analyse et diffuse les données générées par les plaignants et les victimes d'activités frauduleuses. Le Centre appuie les organismes d'enquête et d'application de la loi dans leurs activités de détection et de prévention de la fraude et d'autres crimes économiques et dans les poursuites connexes qu'ils intentent. Comme le Centre héberge des renseignements potentiellement sensibles sur les personnes soupçonnées de fraude et les victimes, le Commissariat a soulevé des préoccupations concernant la possibilité de collecte et de durée de conservation excessives des renseignements.

En se fondant sur nos recommandations, la GRC a accepté de conserver les renseignements personnels des plaignants et des victimes de fraude pendant une période maximale de 10 ans, plutôt que 20 ans, sauf lorsqu'ils sont nécessaires pour des opérations. Elle a également confirmé avoir mis en œuvre nos

recommandations visant à assurer une orientation, une formation et une surveillance internes clairement définies pour faire en sorte que la collecte et l'utilisation des renseignements personnels auxquels le public a accès et qui ont un lien avec les plaintes déposées auprès du Centre soient appropriées.

Secrétariat du Conseil du Trésor du Canada—Norme sur le filtrage de sécurité

Depuis 2011, le Commissariat a sans cesse formulé des conseils et des recommandations au Secrétariat du Conseil du Trésor (SCT) en vue de l'élaboration d'une nouvelle norme sur le filtrage de sécurité, mais le SCT lui a fait parvenir l'EFVP après l'entrée en vigueur de la norme en octobre 2014.

Nous avons constamment exprimé nos préoccupations concernant la portée accrue des processus d'enquête de sécurité, qui donneront lieu à la collecte et à la conservation d'une plus grande quantité de renseignements personnels sensibles. En particulier, nous avons remis en question la nécessité et l'efficacité des vérifications de solvabilité pour tous les postes de la fonction publique, la nécessité et l'exactitude des enquêtes de sources ouvertes ainsi que l'obligation d'effectuer des vérifications des documents sur le respect de la loi (VDAL)—recherche dans les bases de données des constats de police qui est plus exhaustive qu'une vérification du casier judiciaire et qui révèle de l'information sur toute une gamme d'interactions d'un individu avec des organismes d'application de la loi, peu importe s'il a été condamné ou non.

Nous avons informé le SCT qu'il n'avait établi aucun lien entre les objectifs de la Norme et les renseignements personnels recueillis pour chaque mesure imposée par la Norme et qu'il n'avait présenté aucune analyse montrant que chaque mesure exigée était nécessaire et efficace et qu'elle portait le moins possible atteinte à la vie privée.

Le SCT a accepté certaines de nos recommandations, mais il a adopté la Norme sans avoir procédé à une analyse justifiant la collecte et l'utilisation accrues de renseignements personnels. Les ministères ont jusqu'en octobre 2017 pour se conformer entièrement aux exigences de la Norme; cependant, le SCT n'a toujours pas fourni les orientations promises pour la mise en œuvre de cette norme. Nous poursuivons nos discussions avec le SCT dans ce dossier.

COMMUNICATION DE RENSEIGNEMENTS DANS L'INTÉRÊT PUBLIC

Le consentement est au cœur du concept de protection de la vie privée. La capacité d'accorder ou de refuser son consentement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels permet à un individu de protéger son droit à la vie privée.

Par ailleurs, il peut être nécessaire dans des situations particulières de communiquer des renseignements personnels sans le consentement de l'intéressé. Le paragraphe 8(2) de la *Loi sur la protection des renseignements personnels* énonce les situations dans lesquelles les institutions gouvernementales peuvent communiquer des renseignements personnels sans le consentement de l'individu concerné. Entre autres, l'alinéa 8(2)*m*) autorise la communication dans les cas où, de l'avis du responsable de l'institution, des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée ou ceux où l'individu concerné en tirerait un avantage certain.

Il est important de comprendre que ces dispositions de la Loi ne visent pas à gérer la communication régulière ou systématique de renseignements personnels. Elles devraient être invoquées uniquement dans les situations où les institutions fédérales doivent tenir compte de l'intérêt supérieur du public et trouver l'équilibre entre la transparence—le droit de savoir du public—et le droit à la vie privée.

Lorsqu'un ministère ou un organisme fédéral envisage de communiquer des renseignements dans l'intérêt public, il incombe au responsable de l'institution de s'assurer que l'intérêt public l'emporte manifestement sur la protection de la vie privée des individus concernés. Le responsable a aussi l'obligation d'informer le commissaire à la protection de la vie privée de la communication envisagée. Le commissaire n'a pas le pouvoir de mettre fin à la communication de renseignements personnels, mais il peut exprimer ses préoccupations et prévenir la personne dont les renseignements seront communiqués.

En 2016-2017, le Commissariat a été informé de 376 communications faites dans l'intérêt public—89 % des avis venaient de quatre ministères. Les avis comprennent ceux de la GRC aux médias concernant la mise en liberté de délinquants qui présentent un risque élevé de récidive et ceux d'Emploi et Développement social Canada indiquant à la police que des clients ont proféré des menaces de graves préjudices envers eux-mêmes ou d'autres.

Le ministère de la Défense nationale a remis aux proches parents les rapports d'enquête sur le décès de membres des Forces canadiennes. Service correctionnel Canada a déclaré des communications semblables aux proches parents des détenus morts en détention.

COMPARUTIONS DEVANT LE PARLEMENT CONCERNANT LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Le Commissariat à la protection de la vie privée du Canada relève directement du Parlement, auquel il formule des commentaires et des avis relatifs à des questions susceptibles d'avoir une incidence sur le droit à la vie privée des Canadiens.

En 2016-2017, le Commissariat a déposé des mémoires et comparu devant des comités parlementaires concernant plusieurs questions liées à la *Loi sur la protection des renseignements personnels*—notamment en ce qui a trait à la réforme législative, comme il est expliqué plus en détail dans d'autres sections du présent rapport.

Le Commissariat a été prié de procéder à des analyses portant sur d'autres sujets dans la perspective de la protection de la vie privée. Les paragraphes qui suivent en donnent un aperçu.

Projet de loi C-37—Ouvrir le courrier des Canadiens

Dans une comparution devant un comité sénatorial pour analyser le projet de loi C-37, *Loi modifiant la Loi réglementant certaines drogues et autres substances* et apportant des modifications connexes à d'autres lois, le commissaire à la protection de la vie privée a affirmé qu'il serait justifié d'autoriser les agents des douanes et des services frontaliers à ouvrir sans consentement le courrier pesant moins de 30 grammes car des preuves montraient que le système postal international était utilisé pour importer des drogues ayant causé la mort d'un grand nombre de Canadiens. Par contre, le commissaire a aussi indiqué que le projet de loi bénéficierait clairement d'autres mesures pour protéger la vie privée des Canadiens, plus précisément pour s'assurer que la correspondance ne soit pas lue lorsqu'on ne décèle aucun produit de contrebande.

Projet de loi C-226—Étendre le pouvoir de la police d'effectuer des contrôles aléatoires de l'alcoolémie

Parmi les changements proposés au *Code criminel*, le projet de loi C-226, *Loi modifiant le Code criminel (Loi sur la conduite avec facultés affaiblies)*, autoriserait les policiers à ordonner à un conducteur de fournir un échantillon d'haleine en tout temps, même s'ils n'ont aucun motif de soupçonner qu'il a consommé de l'alcool. Tout en affirmant comprendre parfaitement la gravité, l'incidence sociale et les dangers évidents de la conduite avec facultés affaiblies, le commissaire à la protection de la vie privée a suggéré à un comité parlementaire d'analyser l'incidence des changements proposés sur la protection de la vie privée en utilisant un cadre fondé sur des facteurs que la Cour suprême du Canada a pris en compte pour rendre sa décision concernant la constitutionnalité des contrôles aléatoires de l'alcoolémie.

De plus, le commissaire a exprimé ses préoccupations concernant une disposition qui autoriserait la communication des résultats de contrôles aléatoires de l'alcoolémie et autres tests vérifiant la sobriété aux fins de l'application de toute loi fédérale ou provinciale. Il a suggéré au comité de déterminer si les objectifs de ces autres lois sont suffisamment importants pour justifier la communication de renseignements personnels sensibles obtenus sous la contrainte de l'État.

Projet de loi C-4—Publication de renseignements financiers personnels par les syndicats

Le projet de loi C-4, *Loi modifiant le Code canadien du travail,* la *Loi sur les relations de travail au Parlement,* la *Loi sur les relations de travail dans la fonction publique* et la *Loi de l'impôt sur le revenu*, abrogerait le projet de loi C-377, qui obligeait les syndicats à publier le nom, le salaire et d'autres renseignements personnels de certains de leurs employés, y compris des

renseignements sur leurs activités politiques. Au cours d'une comparution devant un comité parlementaire, le commissaire a exprimé son soutien au projet de loi tout en reconnaissant l'importance de la transparence et de la reddition de comptes en tant que principes fondamentaux à la base d'institutions démocratiques solides et efficaces. Il a ainsi réitéré ses inquiétudes au sujet du projet de loi précédent en soulignant qu'il fallait établir un équilibre entre les efforts en faveur de la transparence et la nécessité de protéger les renseignements personnels sensibles. Entre autres, le commissaire a mis en doute l'idée que la transparence assurée en obligeant les syndicats à publier le nom de certains employés et les détails de leurs activités politiques portait atteinte de façon disproportionnée à la vie privée des intéressés.

Projet de loi C-15—Loi nº 1 d'exécution du budget de 2016 (dispositions relatives à la Loi de l'impôt sur le revenu*)*

En plus de percevoir les taxes et impôts, l'Agence du revenu du Canada (ARC) perçoit les sommes dues dans le cadre de certains programmes fédéraux et provinciaux—par exemple, les prêts aux étudiants. La *Loi d'exécution du budget de 2016* modifiait un paragraphe de la *Loi de l'impôt sur le revenu* afin d'autoriser les fonctionnaires de l'ARC qui s'occupent de la perception fiscale à communiquer des « renseignements sur des contribuables » à ceux qui s'occupent du recouvrement de dettes non fiscales. Dans un mémoire présenté à un comité sénatorial chargé d'étudier le projet de loi, le commissaire a indiqué comprendre que ces modifications permettraient d'éviter le double emploi et de simplifier les interactions des particuliers avec l'ARC, en précisant que les renseignements communiqués devraient toutefois se limiter à ceux nécessaires aux fins mentionnées—soit le recouvrement par l'Agence des sommes dues. Une loi ainsi modifiée respecterait la *Loi sur la protection des renseignements personnels.*

Nous avons également exprimé notre point de vue sur une modification qui permettrait la communication de renseignements sur des contribuables au Bureau de l'actuaire en chef uniquement en vue de permettre à ce dernier d'effectuer des révisions actuarielles des régimes de pension établis en vertu de la *Loi sur la sécurité de la vieillesse* conformément aux exigences de la *Loi sur les rapports relatifs aux pensions publiques.*

Nous avons compris que l'intention du gouvernement était de « masquer » ou de désidentifier certains renseignements, ce qui devrait se faire de manière à garantir qu'il sera impossible de les repersonnaliser. L'information partagée ne comprendrait pas tous les renseignements sur les contribuables, mais seulement certaines données se limitant à celles nécessaires pour permettre à l'actuaire en chef de s'acquitter du mandat que lui confère la loi. En outre, des ententes seraient conclues et prévoiraient des mesures de protection de la vie privée limitant la collecte, déterminant des périodes de conservation et établissant des règles pour la destruction des renseignements.

Selon nous, il faut respecter le principe de protection de la vie privée selon lequel la communication d'information devrait être limitée aux renseignements nécessaires pour atteindre les fins prévues. De plus, les ministères qui communiquent les renseignements et le Bureau de l'actuaire en chef, qui les reçoit, devraient conclure des ententes de communication d'information officielles prévoyant des mesures de protection de la vie privée.

Communication d'information à l'Internal Revenue Service (IRS) des États-Unis

En vertu d'une entente conclue en 2014, l'Agence du revenu du Canada recueille auprès d'institutions financières canadiennes des renseignements concernant les comptes détenus par certains Américains et communique ces renseignements à l'Internal Revenue Service. Tout en reconnaissant qu'il est légitime de partager des renseignements pour lutter contre l'évasion fiscale, le commissaire a fait valoir dans une comparution devant le Parlement qu'il faut limiter la collecte d'information à ce qui est nécessaire et imposer des limites similaires à leur utilisation, à leur communication et à leur conservation.

DOSSIERS RELATIFS À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS* DEVANT LES TRIBUNAUX

Au cours de l'exercice, le Commissariat a comparu à maintes reprises devant les tribunaux pour les besoins de plusieurs interventions ou requêtes. Les paragraphes qui suivent en donnent un aperçu.

Procureur général du Canada c. Larry Philip Fontaine et al., CSC 37037 (décision en délibéré)

Le Commissariat est intervenu dans des procédures judiciaires portant sur le sort des dossiers créés dans le cadre du Processus d'évaluation indépendant (PEI) prévu par la Convention de règlement relative aux pensionnats indiens (CRRPI). En tant que partie à la CRRPI, le gouvernement du Canada fait valoir que les dossiers du PEI qu'il détient, lesquels contiennent le récit personnel des abus rapportés par des milliers de survivants des pensionnats, sont des dossiers gouvernementaux et sont par conséquent assujettis à la *Loi sur la protection des renseignements personnels*, à la *Loi sur l'accès à l'information* et à la *Loi sur la Bibliothèque et les Archives du Canada*.

Dans une décision majoritaire rendue en 2016, les juges de la Cour d'appel de l'Ontario ont confirmé la décision d'un tribunal de première instance selon laquelle les dossiers n'appartiennent pas au gouvernement fédéral et qu'il revenait aux survivants des pensionnats eux-mêmes de décider si leurs récits devraient être archivés ou détruits après une période de conservation de 15 ans.

En qualité d'intervenant devant la Cour d'appel, le Commissariat a aidé le tribunal à déterminer si le niveau de protection de la vie privée offert par les lois fédérales sur l'accès à l'information et la protection des renseignements personnels était compatible avec la confidentialité quasi absolue négociée par les parties dans le cadre de la CRRPI. Il a aussi souligné qu'il est important que les survivants des pensionnats exercent un contrôle sur ces renseignements très personnels.

Le Procureur général du Canada a été autorisé à porter la cause en appel devant la Cour suprême du Canada, qui a entendu l'affaire en mai 2017. Le Commissariat est intervenu dans l'appel en déposant des observations écrites.

Syndicat des agents correctionnels du Canada (SACC–CSN) c. Procureur général du Canada, 2016 CF 1289 (décision portée en appel)

Le syndicat a fait valoir devant la Cour fédérale que les vérifications de solvabilité obligatoires pour les agents correctionnels, exigées par la nouvelle *Norme sur le filtrage de sécurité* du Conseil du Trésor, contreviennent à la *Loi sur la protection des renseignements personnels* et à la *Charte canadienne des droits et libertés*.

La Cour a conclu que les renseignements sur la solvabilité peuvent aider à déterminer si un agent est vulnérable à la corruption, si bien qu'il existe un lien direct entre la collecte de renseignements sur la solvabilité d'un agent et le programme de filtrage de sécurité. Cette collecte est donc autorisée en vertu de la *Loi sur la protection des renseignements personnels* et raisonnable pour l'application de la Charte.

En qualité d'intervenant dans la procédure, le Commissariat a fait valoir que, pour éviter toute collecte excessive de renseignements, les institutions gouvernementales doivent montrer que les renseignements personnels qu'elles veulent recueillir sont essentiels à l'exécution efficace d'un programme ou d'une activité, et non simplement utiles ou susceptibles de l'être.

Le commissaire a réitéré ces arguments par la suite dans une lettre adressée au président du Conseil du Trésor et à la ministre de la Justice, en faisant remarquer que la décision de la Cour fédérale souligne l'importance de modifier la *Loi sur la protection des renseignements personnels* afin d'imposer explicitement le critère de nécessité pour la collecte de renseignements personnels, comme c'est le cas dans d'autres lois en la matière au Canada et à l'étranger.

Le syndicat a fait appel de la décision de la Cour fédérale. Le Commissariat a obtenu l'autorisation d'intervenir dans l'appel, qui est en cours.

Oleynik c. Canada (commissaire à la protection de la vie privée), 2016 CF 1167

Dans cette affaire, une personne a déposé une requête à la Cour fédérale en alléguant que le Commissariat lui avait refusé l'accès à des renseignements personnels relevant de lui. La personne a mis en doute l'idée que le Commissariat avait appliqué comme il se doit les différentes exceptions prévues par *Loi sur la protection des renseignements personnels* et que son refus de chercher des renseignements supplémentaires dans les serveurs de sauvegarde était justifié.

La Cour a conclu que les exceptions appliquées par le Commissariat étaient pertinentes dans la grande majorité des cas lorsqu'il a traité les milliers de pages visées par la demande. Elle a aussi validé la décision du Commissariat de ne pas faire de recherches dans les serveurs de sauvegarde, reconnaissant que les renseignements ne pouvaient être « retrouvés sans problèmes sérieux » dans les circonstances.

Alberta (commissaire à l'information et à la protection de la vie privée) c. Université de Calgary, 2016 CSC 53

Le Commissariat à l'information du Canada et plusieurs autres commissariats à l'information et à la protection de la vie privée provinciaux et territoriaux du Canada ont déposé une intervention conjointe devant la Cour suprême du Canada dans un dossier présenté par le commissaire à l'information et à la protection de la vie privée de l'Alberta. Le Commissariat à la protection de la vie privée du Canada et ses cosignataires ont fait valoir que la *Freedom of Information and Protection of Privacy Act* de l'Alberta confère au commissaire de l'Alberta le pouvoir d'exiger l'accès à des documents détenus par une institution publique, comme une université, même si l'institution invoque le secret professionnel de l'avocat—et que ce pouvoir est essentiel pour faire enquête sur les plaintes relatives à l'accès déposées contre des institutions publiques.

La Cour a donné tort au commissaire de l'Alberta, concluant que les lois de la province ne confèrent pas explicitement le pouvoir d'exiger la production de documents à l'égard desquels un organisme public invoque le secret professionnel de l'avocat.

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 *Loi sur la protection des renseignements personnels*, 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 *Loi sur la protection des renseignements personnels*, 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 *Loi sur la protection des renseignements personnels*.

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 *Loi sur la protection des renseignements personnels*, 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 ou des dispositions d'une loi sur la protection des renseignements personnels.

Fondée et résolue :
L'institution ou l'organisation a enfreint une disposition d'une loi sur la protection des renseignements personnels, 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 *Loi sur la protection des renseignements personnels*, 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 *Loi sur la protection des renseignements personnels* : 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

STATISTIQUES RELATIVES À LA LPRPDE

Plaintes en vertu de la LPRPDE acceptées*, par secteur de l'industrie (2016–2017)

Secteur de l'industrie	Nombre de plaintes	Proportion par rapport à l'ensemble des plaintes acceptées**
Finances	79	24 %
Internet	35	11 %
Transports	35	11 %
Services professionnels	33	10 %
Télécommunications	31	10 %
Services	26	8 %
Assurances	19	6 %
Vente et commerce de détail	19	6 %
Autres secteurs	18	6 %
Santé	13	4 %
Hébergement	6	2 %
Gouvernement	6	2 %
Divertissement	5	2 %
Total	**325**	**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 30.

** La somme des composantes peut ne pas être égale au total en raison des écarts d'arrondis.

Plaintes* acceptées en vertu de la LPRDE, par type de plainte (2016–2017)

Type de plainte	Nombre	Proportion par rapport à l'ensemble des plaintes acceptées
Accès	116	36%
Responsabilité	0	0%
Exactitude	13	4%
Fins appropriées	4	1%
Collecte	20	6%
Consentement	79	24%
Correction ou annotation	10	3%
Transparence	5	2%
Conservation	1	0%
Mesures de protection	26	8%
Utilisation et communication	51	16%
Total	**325**	**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 30.

Enquêtes* fermées en vertu de la LPRPDE, par secteur de l'industrie et décision (2016–2017)

Secteur de l'industrie	Règlement rapide	Décision (règlement rapide exclu)									Total partiel des décisions (règlement rapide exclu)	Total des règlements rapides et autres décisions
		Refusée	Abandonnée (art. 12.2)	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue		
Finances	43		8		1		4	1	2		**16**	**59**
Gouvernement	4		2	1			1				**4**	**8**
Sans but lucratif	1										**0**	**1**
Transports	18		2		1					1	**4**	**22**
Télécommunications	20		1		1		1		8		**11**	**31**
Services	23		4			2	2		1		**9**	**32**
Internet	24		8		1					1	**10**	**34**
Autres secteurs	21		5	1	2	1	3	2	3		**17**	**38**
Assurances	10		4				1		3	1	**9**	**19**
Vente et commerce de détail	15				3						**3**	**18**
Hébergement	6		3								**3**	**9**
Services professionnels	17						1			1	**2**	**19**
Divertissement	3							1			**1**	**4**
Total	**205**	**0**	**37**	**2**	**9**	**3**	**13**	**4**	**17**	**4**	**89**	**294**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires (32 plaintes exclues).

Enquêtes* fermées en vertu de la LPRPDE, par type de plainte et décision (2016–2017)

Type de plainte	Règlement rapide	Abandonnée (art. 12.2)	Refusée	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue	Total
Accès	68	2		1	2	3	1	2	7	1	**87**
Utilisation et communication	29	8		1	5		6	2			**51**
Collecte	12	2							1		**15**
Fins appropriées	2								1		**3**
Mesures de protection	16	5					1		2	1	**25**
Consentement	60	16			2		5		2	2	**87**
Exactitude	8								1		**9**
Responsabilité									2		**2**
Correction ou annotation	8	3									**11**
Transparence	1	1									**2**
Détermination des fins de la collecte des renseignements									1		**1**
Conservation	1										**1**
Total	**205**	**37**	**0**	**2**	**9**	**3**	**13**	**4**	**17**	**4**	**294**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires (32 plaintes exclues).

Enquêtes en vertu de la LPRPDE (2016–2017)—Délais de traitement moyens, par décision (enquêtes*)

Décision	Nombre	Délai de traitement moyen en mois
Résolue par règlement rapide	205	2,6
Réglée	3	7,0
Abandonnée (art. 12.2)	37	5,5
Retirée	9	8,0
Hors du champ d'application	2	12,0
Non fondée	13	14,3
Fondée et conditionnellement résolue	4	21,6
Fondée et résolue	17	18,3
Fondée	4	13,4
Nombre total de cas	**294**	
Moyenne générale pondérée		**5,1**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires (32 plaintes exclues).

Enquêtes* en vertu de la LPRPDE (2016–2017)—délais de traitement moyens, par type de plainte et règlement

	Règlement rapide		Autre règlement (sauf règlement rapide)		Toutes les enquêtes	
Type de plainte	Nombre de cas	Délai de traitement moyen en mois	Nombre de cas	Délai de traitement moyen en mois	Nombre de cas	Délai de traitement moyen en mois
Accès	68	2,7	19	15,5	87	5,5
Responsabilité			2	18,5	2	18,5
Exactitude	8	2,5	1	7,6	9	3,1
Fins appropriées	2	4,7	1	12,7	3	7,3
Collecte	12	2,1	3	6,3	15	2,9
Consentement	60	2,5	27	11,0	87	5,1
Correction ou annotation	8	3,3	3	5,2	11	3,8
Conservation	1	2,4			1	2,4
Détermination des fins de la collecte des renseignements			1	7,4	1	7,4
Transparence	1	3,4	1	8,0	2	5,7
Mesures de protection	16	2,2	9	7,3	25	4,0
Utilisation et communication	29	2,9	22	8,7	51	5,4
Total	**205**	**2,6**	**89**	**10,7**	**294**	**5,1**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires (32 plaintes exclues).

Déclarations volontaires des atteintes en vertu de la LPRPDE, par secteur de l'industrie et type d'incident (2016–2017)

Secteur de l'industrie	Type d'incident			Total des incidents par secteur de l'industrie	Proportion par rapport à l'ensemble des incidents*
	Communication accidentelle	Perte	Vol et accès non autorisé		
Hébergement	1			**1**	**1 %**
Divertissement	1		3	**4**	**4 %**
Finances	15		9	**24**	**25 %**
Santé	4	1	2	**7**	**7 %**
Assurances	4			**4**	**4 %**
Internet			10	**10**	**11 %**
Organismes sans but lucratif	2		7	**9**	**9 %**
Autres secteurs	2		8	**10**	**11 %**
Vente et commerce de détail	1		7	**8**	**8 %**
Services	3	3	6	**12**	**13 %**
Télécommunications	3		3	**6**	**6 %**
Total	**36**	**4**	**55**	**95**	**100 %**

* La somme des composantes peut ne pas être égale au total en raison des écarts d'arrondis.

TABLEAUX STATISTIQUES LIÉS À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

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

Intimé	Fondée	Fondée et résolue	Non fondée	Hors du champ d'application	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
Affaires autochtones et du Nord Canada		1	1		1	1			**4**
Affaires mondiales Canada			1		1		9		**11**
Agence canadienne d'inspection des aliments						1			**1**
Agence de la santé publique du Canada						1	6		**7**
Agence des services frontaliers du Canada	6		9		1	2	40		**58**
Agence du revenu du Canada		6	7				30		**43**
Agence Parcs Canada							4		**4**
Agriculture et Agroalimentaire Canada							2		**2**
Anciens Combattants Canada			2				4		**6**
Banque du Canada						1	1		**2**
Bibliothèque et Archives Canada							4		**4**
Bureau du Conseil privé								1	**1**
Centre de la sécurité des télécommunications Canada							1	1	**2**
Comité de surveillance des activités de renseignement de sécurité							2		**2**
Commissariat aux langues officielles			1						**1**
Commission canadienne des droits de la personne						1			**1**
Commission de la fonction publique du Canada						3			**3**
Commission de l'immigration et du statut de réfugié du Canada							1		**1**
Commission des libérations conditionnelles du Canada	2	1	4				10		**17**
Conseil canadien des normes			1						**1**
Conseil de la radiodiffusion et des télécommunications canadiennes			2						**2**
Conseil de recherches en sciences humaines du Canada			1						**1**
Conseil national de recherches Canada		1					1		**2**

Intimé	Fondée	Fondée et résolue	Non fondée	Hors du champ d'application	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
École de la fonction publique du Canada		1							**1**
Emploi et Développement social Canada			2			3	14		**19**
Environnement et Changement climatique Canada							10		**10**
Gendarmerie royale du Canada	2	1	13		1	5	63	1	**86**
Immigration, Réfugiés et Citoyenneté Canada		1	1			15	16	1	**34**
Innovation, Sciences et Développement économique Canada		1				1	3		**5**
Marine Atlantique S.C.C.							1		**1**
Ministère de la Défense nationale	3	3	9			2	34		**51**
Ministère de la Justice du Canada			4			2	2		**8**
Ministère des Finances Canada			1				1		**2**
Office national de l'énergie		1				1			**2**
Patrimoine canadien							1		**1**
Pêches et Océans Canada							2		**2**
Ressources naturelles Canada			2	1	1	1	2	1	**8**
Revera Inc.		1							**1**
Santé Canada	1					2	4		**7**
Secrétariat du Conseil du Trésor du Canada		1				2	1		**4**
Service canadien du renseignement de sécurité			15				9		**24**
Service correctionnel Canada	3	3	15		2	4	67	9	**103**
Service des poursuites pénales du Canada		1					3		**4**
Service Canada			2		2		2		**6**
Services partagés Canada							1		**1**
Services publics et Approvisionnement Canada			1			2	10		**13**
Société canadienne des postes	3		1			1	12		**17**
Société Radio-Canada							3		**3**
Statistique Canada							12		**12**
Transports Canada						1	2		**3**
Tribunal des anciens combattants (révision et appel)							2		**2**
Total	**20**	**23**	**95**	**1**	**9**	**52**	**392**	**14**	**606**

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	**245**	**3,75**
Accès	234	3,81
Correction ou annotation	8	3,19
Refus d'accès	1	0,67
Langue	2	2,43
Délais	**32**	**0,59**
Protection des renseignements personnels	**146**	**4,46**
Utilisation et communication	101	4,88
Collecte	28	3,58
Conservation et retrait	14	3,59
Exactitude	3	2,54
Total	**423**	**3,76**

Délais de traitement des plaintes en vertu de la LPRP—Enquêtes régulières, par type de plainte

Type de plainte	Nombre	Délai de traitement moyen en mois
Accès	144	18,56
Accès	136	18,76
Correction ou annotation	2	14,10
Langue	6	15,59
Délais	445	5,22
Délais	399	5,27
Correction—délais	5	9,80
Avis de prorogation	41	4,16
Protection des renseignements personnels	71	20,80
Utilisation et communication	51	22,22
Collecte	16	16,50
Conservation et retrait	2	17,92
Exactitude	2	21,94
Total	**660**	**9,80**

Délais de traitement en vertu de la LPRP—Tous les dossiers fermés, par décision

Type de plainte	Nombre	Délai de traitement moyen en mois
Plaintes ordinaires	**660**	**9,80**
Fondées	412	5,94
Non fondées	119	15,22
Abandonnées	77	11,44
Fondées et résolues	25	32,17
Réglées	14	17,03
Hors du champ d'application	3	10,85
Résolues	10	25,66
Résolues par règlement rapide	**423**	**3,76**
Total *	**1 083**	**7,44**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 4 685.

Atteintes en vertu de la LPRP, par institution

Intimé	Incident
Affaires autochtones et du Nord Canada	4
Affaires mondiales Canada	10
Agence canadienne d'inspection des aliments	1
Agence de la santé publique du Canada	1
Agence du revenu du Canada	10
Anciens Combattants Canada	1
Centre de la sécurité des télécommunications Canada	1
Commission de la fonction publique Canada	3
Commission des libérations conditionnelles du Canada	1
Défense nationale	1
Emploi et Développement social Canada	45
Gendarmerie royale du Canada	14
Immigration, Réfugiés et Citoyenneté Canada	8
Instituts de recherche en santé du Canada	1
Pêches et Océans Canada	2
Ressources naturelles Canada	1
Revera Inc.	1
Santé Canada	3
Secrétariat du Conseil du Trésor du Canada	2
Sécurité publique Canada	3
Service correctionnel Canada	12
Service des poursuites pénales du Canada	2
Services partagés Canada	1
Services publics et Approvisionnement Canada	9
Société Radio-Canada	2
Statistique Canada	3
Transports Canada	5
Total	**147**

Plaintes et atteintes en vertu de la *Loi sur la protection des renseignements personnels*

Plaintes en vertu de la *Loi sur la protection des renseignements personnels* (2016–2017)

Catégorie	Total
Acceptées	
Accès	424
Délais	619
Protection des renseignements personnels	314
Total - plaintes acceptées*	**1 357**
Fermées à la suite d'un processus de règlement rapide	
Accès	245
Délais	32
Protection des renseignements personnels	146
Total	**423**
Fermées à la suite d'une enquête régulière	
Accès	144
Délais	445
Protection des renseignements personnels	71
Total	**660**
Nombre total de dossiers fermés†	**1 083**
Plaintes pour atteinte reçues	
Communication accidentelle	87
Vol	4
Perte	45
Accès non autorisé	11
Total†—Plaintes reçues	**147**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 2 152.

† Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 4 685

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

Type de plainte	Règlement rapide		Enquête		Nombre total	Pourcentage total**
	Nombre	Pourcentage	Nombre	Pourcentage		
Accès						
Accès	251	50 %	154	18 %	**405**	**30 %**
Correction ou annotation	7	1 %	4	0 %	**11**	**1 %**
Refus d'accès	1	0 %	0	0 %	**1**	**0 %**
Langue	5	1 %	2	0 %	**7**	**1 %**
Délais						
Délais	32	6 %	544	64 %	**576**	**42 %**
Prorogation	0	0 %	41	5 %	**41**	**3 %**
Correction—délais	0	0 %	2	0 %	**2**	**0 %**
Protection des renseignements personnels						
Utilisation et communication	139	28 %	73	9 %	**212**	**16 %**
Collecte	40	8 %	30	4 %	**70**	**5 %**
Conservation et retrait	21	4 %	4	0 %	**25**	**2 %**
Exactitude	5	1 %	2	0 %	**7**	**1 %**
Total	**501**	**100 %**	**856**	**100 %**	**1 357**	**100 %**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 2 152.

** La somme des composantes peut ne pas être égale au total en raison des écarts d'arrondis.

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

Intimé	Accès		Délais		Protection des renseignements personnels		Total
	Règlement rapide	Enquête	Règlement rapide	Enquête	Règlement rapide	Enquête	
Service correctionnel du Canada	34	27	13	286	24	13	**397**
Gendarmerie royale du Canada	43	16	2	61	16	24	**162**
Défense nationale	42	6	4	78	10	7	**147**
Agence des services frontaliers du Canada	29	6	5	40	18	9	**107**
Agence du revenu du Canada	17	4	2	21	17	4	**65**
Immigration, Réfugiés et Citoyenneté Canada	10	11	1	22	14	2	**60**
Emploi et Développement social Canada	9	4	1	9	9	4	**36**
Commission d'examen des plaintes concernant la police militaire	0	12	0	16	7	14	**49**
Service canadien du renseignement de sécurité	13	17	0	0	0	0	**30**
Services publics et Approvisionnement Canada	2	3	1	8	10	1	**25**
Total*	**199**	**106**	**29**	**541**	**125**	**78**	**1 078**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 52.

Les 10 institutions visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP (2016–2017), par exercice financier

Organisation	2013-2014	2014-2015	2015-2016	2016-2017
Service correctionnel du Canada	514	314	547	397
Gendarmerie royale du Canada	265	140	120	162
Défense nationale	84	68	77	147
Agence des services frontaliers du Canada	56	66	88	107
Agence du revenu du Canada	61	106	85	65
Immigration, Réfugiés et Citoyenneté Canada	53	42	44	60
Emploi et Développement social Canada	78	35	42	36
Commission d'examen des plaintes concernant la police militaire	0	0	0	49
Service canadien du renseignement de sécurité	17	21	31	30
Services publics et Approvisionnement Canada	13	9	10	25
Total	**1 141**	**801**	**1 044**	**1 078**

Plaintes acceptées en vertu de la LPRP, par institution

Intimé	Règlement rapide	Enquête	Total
Administration canadienne de la sûreté du transport aérien	0	2	**2**
Affaires autochtones et du Nord Canada	0	2	**2**
Affaires mondiales Canada	7	2	**9**
Agence canadienne d'inspection des aliments	1	2	**3**
Agence de la santé publique du Canada	4	0	**4**
Agence des services frontaliers du Canada	52	55	**107**
Agence du revenu du Canada	36	29	**65**
Agence Parcs Canada	2	1	**3**
Agriculture et Agroalimentaire Canada	2	0	**2**
Anciens Combattants Canada	8	5	**13**
Banque du Canada	2	1	**3**
Bibliothèque et Archives Canada	2	1	**3**
Bureau de l'enquêteur correctionnel	0	1	**1**
Bureau du Conseil privé	0	2	**2**
Centre d'analyse des opérations et déclarations financières du Canada	0	1	**1**
Centre de la sécurité des télécommunications Canada	1	0	**1**
Comité de surveillance des activités de renseignement de sécurité	0	1	**1**
Comité externe d'examen de la GRC	0	5	**5**
Commissaire à l'intégrité du secteur public du Canada	0	1	**1**
Commissariat à l'information du Canada	1	0	**1**
Commissariat aux langues officielles	0	5	**5**
Commission canadienne des droits de la personne	3	3	**6**
Commission de la fonction publique du Canada	6	9	**15**
Commission de l'immigration et du statut de réfugié du Canada	5	0	**5**
Commission des libérations conditionnelles du Canada	11	4	**15**
Commission des relations de travail et de l'emploi dans la fonction publique	1	0	**1**
Commission d'examen des plaintes concernant la police militaire	7	42	**49**
Conseil canadien des relations industrielles	0	1	**1**
Conseil de la radiodiffusion et des télécommunications canadiennes	0	2	**2**
Conseil de recherches en sciences humaines du Canada	0	1	**1**
Conseil national de recherches Canada	3	0	**3**
Emploi et Développement social Canada	19	17	**36**
Environnement et Changement climatique Canada	2	8	**10**

Intimé	Règlement rapide	Enquête	Total
Gendarmerie royale du Canada	61	101	**162**
Immigration, Réfugiés et Citoyenneté Canada	25	35	**60**
Innovation, Sciences et Développement économique Canada	4	2	**6**
Marine Atlantique S.C.C.	1	0	**1**
Ministère de la Défense nationale	56	91	**147**
Ministère de la Justice du Canada	3	10	**13**
Ministère des Finances Canada	1	4	**5**
Musée canadien de l'histoire	1	0	**1**
Office des transports du Canada	0	1	**1**
Office national de l'énergie	1	1	**2**
Patrimoine canadien	1	1	**2**
Pêches et Océans Canada	5	9	**14**
Ressources naturelles Canada	3	6	**9**
Santé Canada	5	7	**12**
Secrétariat du Conseil du Trésor du Canada	2	5	**7**
Sécurité publique Canada	1	1	**2**
Service canadien d'appui aux tribunaux administratifs	0	1	**1**
Service canadien du renseignement de sécurité	13	17	**30**
Service correctionnel Canada	71	326	**397**
Service des poursuites pénales du Canada	4	3	**7**
Service Canada	3	3	**6**
Services partagés Canada	1	0	**1**
Services publics et Approvisionnement Canada	13	12	**25**
Société canadienne des postes	16	3	**19**
Société canadienne d'hypothèque et de logement	1	0	**1**
Société Radio-Canada	2	0	**2**
Statistique Canada	21	1	**22**
Technologies du développement durable du Canada	1	2	**3**
Transports Canada	6	11	**17**
Tribunal des anciens combattants (révision et appel)	2	0	**2**
VIA Rail Canada	2	0	**2**
Total*	**501**	**856**	**1 357**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 2 152.

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

Province ou territoire	Règlement rapide		Enquête		Nombre total	Pourcentage total
	Nombre	Pourcentage	Nombre	Pourcentage		
Alberta	36	2,65 %	80	5,90 %	**116**	**8,55 %**
Autre (sauf É.-U.)	6	0,44 %	4	0,29 %	**10**	**0,74 %**
Colombie-Britannique	101	7,44 %	144	10,61 %	**245**	**18,05 %**
États-Unis	3	0,22 %	0	0,00%	**3**	**0,22 %**
Île-du-Prince-Édouard	0	0,00 %	1	0,07 %	**1**	**0,07 %**
Manitoba	21	1,55 %	18	1,33 %	**39**	**2,87 %**
Non précisé	5	0,37 %	0	0,00 %	**5**	**0,37 %**
Nouveau-Brunswick	13	0,96 %	42	3,10 %	**55**	**4,05 %**
Nouvelle-Écosse	13	0,96 %	30	2,21 %	**43**	**3,17 %**
Nunavut	1	0,07 %	0	0,00 %	**1**	**0,07 %**
Ontario	212	15,62 %	362	26,68 %	**574**	**42,30 %**
Québec	71	5,23 %	148	10,91 %	**219**	**16,14 %**
Saskatchewan	16	1,18 %	21	1,55 %	**37**	**2,73 %**
Terre-Neuve-et-Labrador	2	0,15 %	3	0,22 %	**5**	**0,37 %**
Territoires du Nord-Ouest	0	0,00 %	0	0,00 %	**0**	**0,00 %**
Yukon	0	0,00 %	0	0,00 %	**0**	**0,00 %**
Vide	1	0,07 %	3	0,22 %	**4**	**0,29 %**
Total*	**501**	**36,92 %**	**856**	**63,08 %**	**1 357**	**100,00 %**

* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 2 152.

Décisions en vertu de la LPRP, par type de plainte

Type de plainte	Fondée	Fondée et résolue	Non fondée	Hors du champ d'application	Résolue	Abandonnée	Résolue par règlement rapide	Réglée	Total
Accès									
Accès	5	23	67	1	6	28	234	6	**370**
Correction ou annotation			1		1		8		**10**
Refus d'accès							1		**1**
Langue							2	6	**8**
Délais									
Délais	361	1	14	1		22	32		**431**
Prorogation	29	1	9	1		1			**41**
Correction - délais	2		1			2			**5**
Protection des renseignements personnels									
Utilisation et communication	12		22		2	13	101	2	**152**
Collecte	2		4		1	9	28		**44**
Conservation et retrait						2	14		**16**
Exactitude	1		1				3		**5**
Total *	**412**	**25**	**119**	**3**	**10**	**77**	**423**	**14**	**1 083**

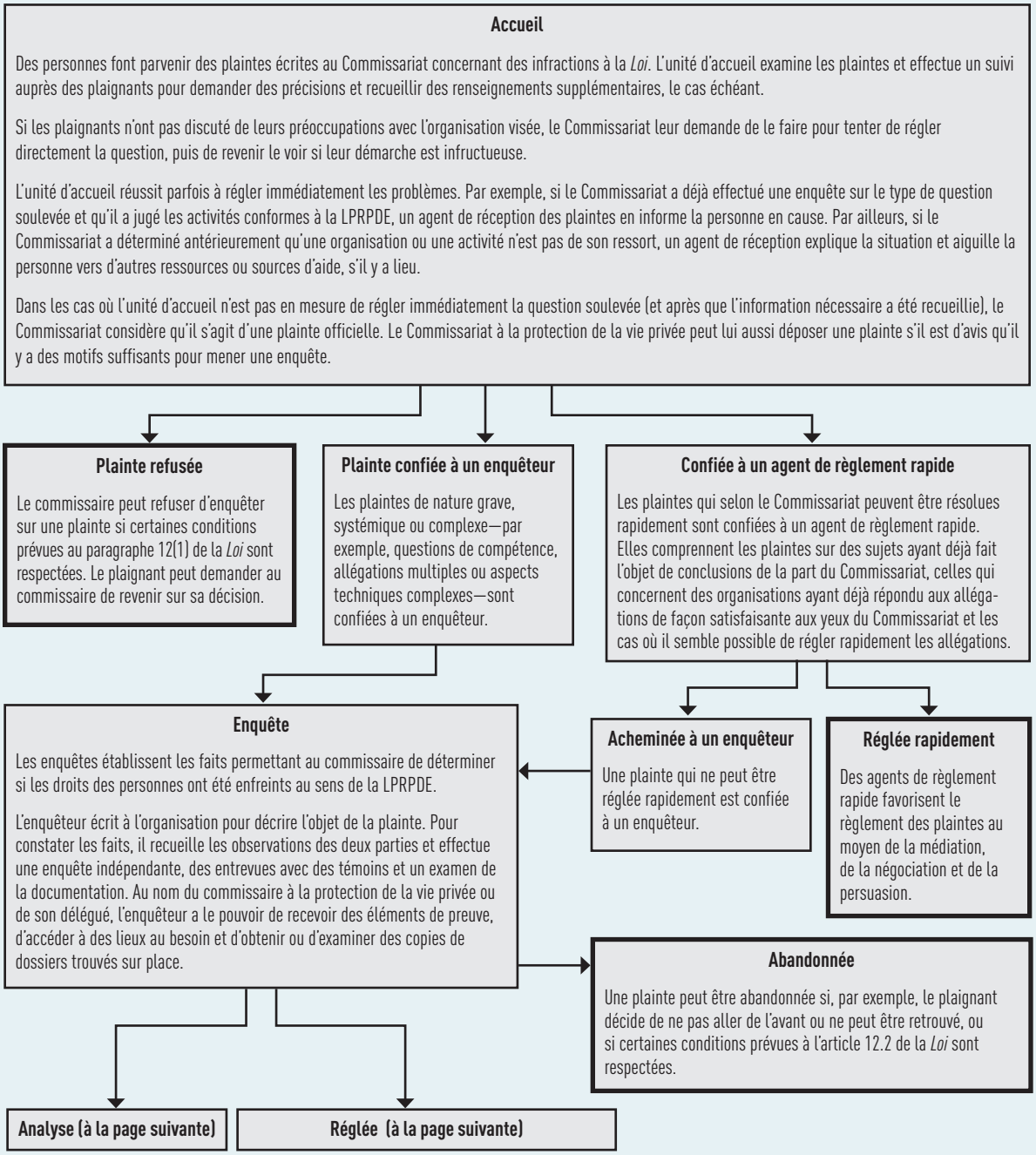
* Comprend une plainte représentative pour chaque série de plaintes similaires et de plaintes déposées par un petit nombre de plaignants individuels; le total des plaintes exclues équivaut à 4 685.

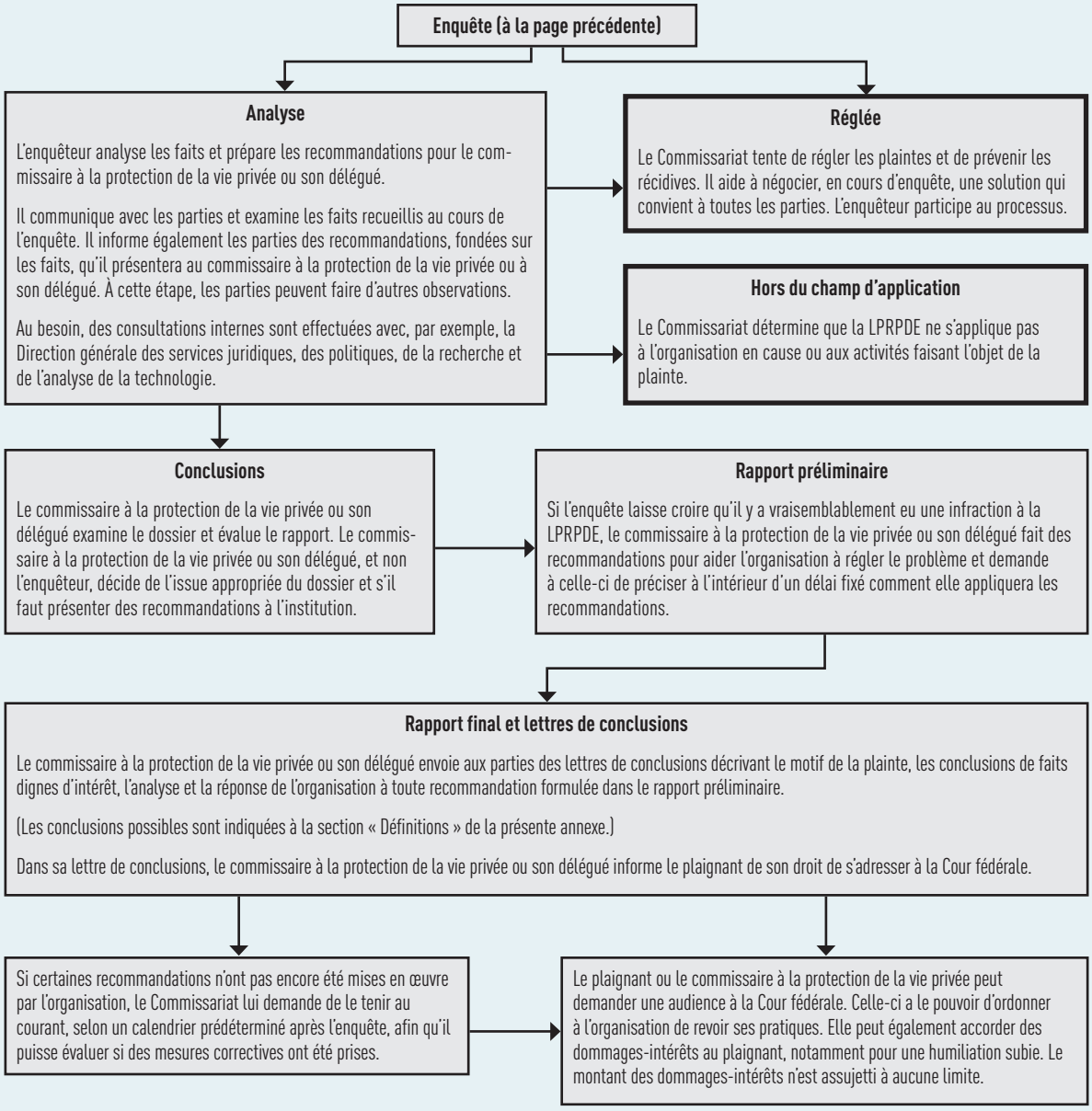
Décisions sur les plaintes relatives aux délais en vertu de la LPRP, par institution

Intimé	Fondée	Fondée et résolue	Non fondée	Hors du champ d'application	Résolue	Abandonnée	Résolue par règlement rapide	Total
Affaires mondiales Canada	2							**2**
Agence des services frontaliers du Canada	27		1			6	5	**39**
Agence du revenu du Canada	20		1			1	2	**24**
Comité de surveillance des activités de renseignement de sécurité	1							**1**
Comité externe d'examen de la GRC			2					**2**
Commission de la fonction publique	1					2		**3**
Commission des libérations conditionnelles du Canada	1							**1**
Commission d'examen des plaintes concernant la police militaire	16							**16**
Conseil canadien des relations industrielles	1							**1**
École de la fonction publique du Canada	2							**2**
Emploi et Développement social Canada	8						1	**9**
Environnement et Changement climatique Canada	1		2					**3**
Gendarmerie royale du Canada	36	2	2	2			2	**44**
Immigration, Réfugiés et Citoyenneté Canada	18		1			1	1	**21**
Innovation, Sciences et Développement économique Canada			1				1	**2**
Ministère de la Défense nationale	71		4			2	4	**81**
Ministère de la Justice du Canada	1		1					**2**
Ministère des Finances Canada	4							**4**
Office de commercialisation du poisson d'eau douce						1		**1**
Patrimoine canadien	1							**1**
Pêches et Océans Canada							2	**2**
Ressources naturelles Canada	3							**3**
Santé Canada	2							**2**
Secrétariat du Conseil du Trésor du Canada	1		2			2		**5**
Service correctionnel Canada	171		5			10	13	**199**
Service des poursuites pénales	2							**2**
Services publics et Approvisionnement Canada	1						1	**2**
Société canadienne des postes			1					**1**
Transports Canada	1		1					**2**
Total	**392**	**2**	**24**	**2**	**0**	**25**	**32**	**477**

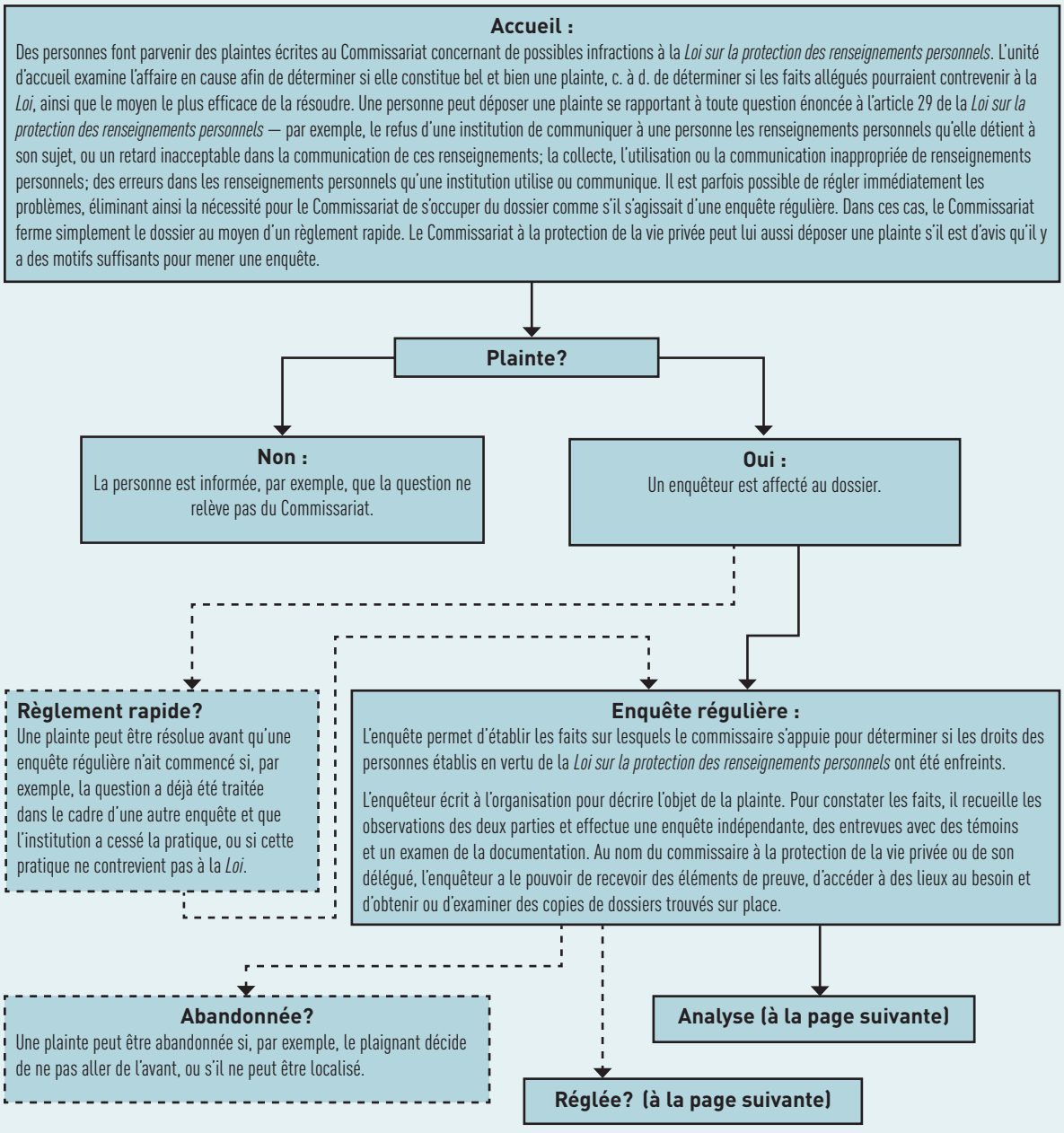
Annexe 3—Processus d'enquête

PROCESSUS D'ENQUÊTE EN VERTU DE LA LPRPDE

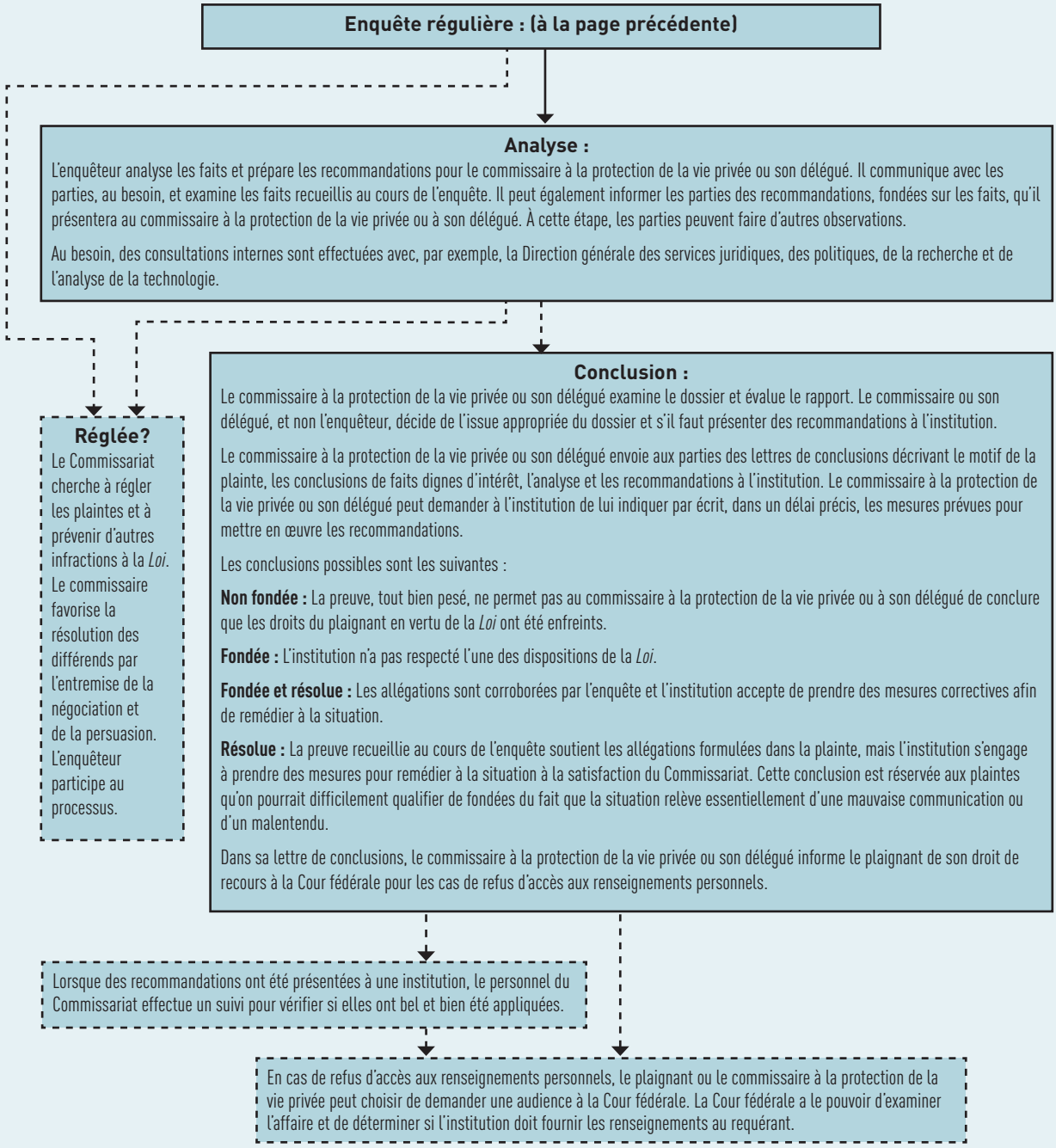



Enquête (à la page précédente)
Analyse
L'enquêteur analyse les faits et prépare les recommandations pour le commissaire à la protection de la vie privée ou son délégué.
Il communique avec les parties et examine les faits recueillis au cours de l'enquête. Il informe également les parties des recommandations, fondées sur les faits, qu'il présentera au commissaire à la protection de la vie privée 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 générale des services juridiques, des politiques, de la recherche et de l'analyse de la technologie.
Réglée
Le Commissariat tente de régler les plaintes et de prévenir les récidives. 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 à la protection de la vie privée ou son délégué examine le dossier et évalue le rapport. Le commissaire à la protection de la vie privée ou son délégué, et non l'enquêteur, décide de l'issue appropriée du dossier et s'il faut présenter des recommandations à l'institution.
Rapport préliminaire
Si l'enquête laisse croire qu'il y a vraisemblablement eu une infraction à la LPRPDE, le commissaire à la protection de la vie privée ou son délégué fait des recommandations pour aider l'organisation à régler le problème et demande à celle-ci de préciser à l'intérieur d'un délai fixé comment elle appliquera les recommandations.
Rapport final et lettres de conclusions
Le commissaire à la protection de la vie privée 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 la section « Définitions » de la présente annexe.)
Dans sa lettre de conclusions, le commissaire à la protection de la vie privée ou son délégué informe le plaignant de son droit de s'adresser 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, selon un calendrier prédéterminé après l'enquête, afin qu'il puisse évaluer si des mesures correctives ont été prises.
Le plaignant ou le commissaire à la protection de la vie privée peut 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 assujetti à aucune limite.

PROCESSUS D'ENQUÊTE EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*



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



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

Annexe 4 – Rapport du commissaire spécial à la protection de la vie privée pour 2016–2017

J'ai le plaisir de rendre compte des activités du bureau du commissaire spécial à la protection de la vie privée dans le présent rapport. Depuis le 1er avril 2007, le Commissariat à la protection de la vie privée du Canada (CPVP) est assujetti à la *Loi sur la protection des renseignements personnels.* Il peut donc recevoir des demandes de renseignements personnels du fait qu'il s'agit d'une institution à laquelle s'applique le droit d'accès à ce type de renseignements.

La loi qui a apporté cette modification n'a toutefois prévu aucun mécanisme distinct de celui relevant du CPVP pour l'examen des plaintes selon lesquelles le CPVP n'aurait pas traité une demande de renseignements personnels conformément à la loi. Compte tenu d'un principe essentiel du droit de l'accès à l'information qui veut que les décisions sur la communication des renseignements gouvernementaux fassent l'objet d'un examen indépendant, on a créé le poste de commissaire spécial à la protection de la vie privée qui a le pouvoir d'enquêter sur les plaintes relatives au CPVP.

C'est pourquoi le commissaire m'a délégué la majorité des pouvoirs et des attributions qui lui sont dévolus en vertu des articles 29 à 35 et de l'article 42 de la Loi pour me permettre d'examiner les plaintes déposées contre le CPVP sous le régime de la Loi.

Plaintes de l'exercice précédent non réglées

Une plainte déposée au cours de l'exercice précédent n'était toujours pas réglée. Cette plainte a été déposée par un individu qui soutenait que le CPVP n'avait pas fourni tous les documents dans sa réponse. L'enquête que j'ai menée a permis de conclure que tous les documents ont bel et bien été fournis.

Nouvelles plaintes déposées au cours du présent exercice

Quatre plaintes ont été reçues cette année; elles ont toutes fait l'objet d'une enquête et ont été réglées avant la fin de l'exercice.

Les questions soulevées dans deux plaintes visent la perte de renseignements personnels dans des envois postaux envoyés au CPVP. Dans les deux plaintes, la perte de renseignements personnels s'est produite dans la salle du courrier. Cette dernière était aménagée d'une façon telle que le courrier pouvait se retrouver dans des bacs dont le contenu allait être déchiqueté. L'enquête que j'ai menée a permis de conclure que l'on ne pouvait déterminer avec certitude ce qui était arrivé aux deux pièces de correspondance perdues, mais que l'explication la plus vraisemblable était qu'elles avaient été déchiquetées par erreur. J'étais satisfait des mesures que le CPVP avait prises pour éviter que cela ne se reproduise à l'avenir. Par conséquent, j'ai conclu que ces plaintes étaient fondées et résolues.

L'une des plaintes concernait l'application des dispositions du paragraphe 22.1(1) de la Loi, selon lesquelles le CPVP est exempté de communiquer les renseignements obtenus ou préparés dans le cadre d'une enquête.

Cependant, une fois l'enquête et toutes les procédures connexes terminées, cette exemption est levée en partie; elle ne s'applique plus aux documents créés par le CPVP durant l'enquête.

Mon enquête a révélé que les documents contestés avaient été obtenus au cours des propres enquêtes du CPVP. J'ai donc conclu que l'organisme avait appliqué cette exception obligatoire à juste titre lorsqu'il avait refusé de communiquer les documents demandés.

La quatrième plainte a été déposée par un individu qui soutenait que le CPVP avait communiqué de manière inappropriée des renseignements personnels le concernant. Des détails au sujet d'une rencontre en personne ont été diffusés au sein du CPVP par inadvertance pendant une brève période de temps, ce qui a permis à un petit nombre de personnes de prendre connaissance de ces renseignements. Même si j'ai conclu que la plainte était fondée, j'ai également déterminé que la divulgation avait été involontaire.

Outre ces quatre plaintes, le commissaire spécial a reçu de la correspondance d'un certain nombre de personnes qui n'étaient pas satisfaites de la manière dont le CPVP avait traité leurs plaintes concernant d'autres institutions ou le temps consacré au traitement de ces plaintes. Le commissaire spécial n'a pas compétence pour enquêter au sujet des préoccupations concernant la façon dont le CPVP a mené enquête sur des plaintes qui lui ont été présentées à titre d'organe de surveillance en vertu de la Loi. En outre, mon bureau ne peut pas non plus enquêter au sujet du temps pris par le CPVP pour traiter de telles plaintes. Notre mandat se limite à recevoir des plaintes selon lesquelles le CPVP aurait mal géré lui-même les renseignements personnels dont il a la garde, et à faire enquête sur ces plaintes.

Conclusion

L'existence du commissaire spécial, qui occupe une fonction indépendante, permet de veiller à l'intégrité du traitement des demandes présentées au CPVP, en tant qu'institution, et contribue ainsi à l'application correcte de la Loi. Mon bureau continuera de jouer ce rôle.

Le tout respectueusement soumis,

David Loukidelis, c.r.
Commissaire spécial pour le
Commissariat à la protection de la vie privée du Canada

Mai 2017